RESERVADO **ME 11-1**

EJÉRCITO DEL PERÚ

COMUNICACIONES

DOCTRINA GENERAL
DE
TELEMÁTICA

MAY – 2004

MANUAL DEL EJERCITO MINISTERIO DE DEFENSA

Chorrillos, 01 de Mayo del 2004

COMUNICACIONES
DOCTRINA GENERAL DE TELEMÁTICA

CAPITULO 1
GENERALIDADES

SECCIÓN I. INTRODUCCION

01. FINALIDAD

a. Este manual intenta constituirse en el fundamento doctrinario del apoyo de Telemática en el ejército, consistente con la doctrina contenida en el ME 11-13 (Operaciones de Información, ed 1999); expandiéndola en sus aspectos pertinentes a Telemática. Esta publicación contiene la guía general necesaria sobre el apoyo de Telemática, para que los comunicantes apoyen a los combatientes en la ejecución de todo el rango de operaciones militares.

b. Proporciona también la doctrina básica de Telemática para apoyar a una fuerza designada, al desarrollo de combate, a la educación profesional de los comunicantes y a su entrenamiento; estableciéndose y reiterándose que un apoyo de Telemática efectivo será vital para el cumplimiento de la misión de combate.

c. Finalmente establece las bases para el desarrollo doctrinario de los conceptos siguientes:
   (1) Apoyo de Telemática a las operaciones de información
   (2) Administración de redes y sistemas de comando y control táctico.
   (3) Planeamiento del empleo, despliegue y administración de redes de equipos terminales móviles de usuarios.
   (4) Otros sistemas de comunicaciones y de distribución de datos que se indican.

02. ALCANCE

a. El contenido de este manual está basado en experiencias operacionales propias y de otros ejércitos victoriosos donde el apoyo de Telemática fue esencial para su éxito, así como en conceptos de actualidad en la era de la información e iniciativas pragmáticas que visan la modernización de comunicaciones, particularmente la digitalización de todo su equipamiento.

b. Este manual está dirigido a todos los comandos de los diferentes escalones, a los Estados Mayores y personal militar en general, que de manera directa o indirecta tengan que ver con el apoyo de Telemática a las operaciones militares del ejército; examinando como los nuevos conceptos de telecomunicaciones, automatización, protección y diseño de sistemas de información, la estructura de las fuerzas y hasta las responsabilidades de los usuarios han cambiado el rol de los comunicantes en su apoyo a las operaciones del ejército.

03. ASPECTOS CONCEPTUALES INTRODUCTORIOS SOBRE EL APOYO DE TELEMÁTICA

a. El apoyo de Telemática en todos los escalones, en un campo de batalla moderno, es un factor importante del planeamiento y ejecución de operaciones no sólo dentro del ejército, sino en las fuerzas armadas; ya que las comunicaciones, como una de sus disciplinas fundamentales, son

esenciales en la integración y sincronización de las fuerzas, desde la preparación de las mismas hasta la ejecución de las operaciones planeadas.

b. El apoyo de Telemática consiste de una serie de disciplinas que administran la información, proporcionando redes y sistemas colectivos, integrados y sincronizados que apoyan a las capacidades del combatiente a través de todo el rango de las operaciones militares, para permitir que los comandantes en todos los escalones alcancen sus objetivos y conduzcan con éxito sus campañas, sus operaciones estratégicas – operativas, sus operaciones tácticas y sus combates y/o encuentros; buscando asegurar la obtención de la superioridad del ciclo de toma de decisiones de comando y control.
c. El apoyo de Telemática implementa los aspectos conceptuales de la tecnología de la información y administración de la información, en apoyo a las operaciones de informaciones (OI) en los niveles de la guerra estratégicos y tácticos, en las operaciones especiales y hasta en contingencias de escalas más pequeñas.
d. En la era de la información, viene siendo evidente la creciente dependencia de las unidades y organizaciones del ejército en la conectividad electrónica, más que en la conectividad geográfica o física; por lo tanto los comunicantes deberán usar y sentir confianza en que la información y la tecnología dominará, controlará y ganará combates y guerras en los campos de batalla modernos.
e. Aunque el contexto actual regional latinoamericano, nos señala que los peligros y amenazas de una guerra entre naciones vecinas se ha alejado, han surgido otras situaciones conflictivas o de tensión que obligarán al empleo de las fuerzas del ejército; derivadas de nacionalismos regionales, afanes separatistas, fervores religiosos e ideológicos, competencias económicas, entre otras causas, que contribuirán a la inestabilidad regional; surgiendo de esta manera otras amenazas como el tráfico ilícito de drogas, el terrorismo, riesgos contra el flujo de info y sistemas de información, operaciones militares convencionales de escala focalizada, etc. Todas estas nuevas amenazas, tendrán diferentes motivaciones y niveles de sofisticación en su armamento, tecnología y capacidades de comando, control, comunicaciones e inteligencia (C^3I).
f. Para contrarrestar estas amenazas se necesitará establecer el dominio de la información y poder de fuegos sobre cualquier adversario y sobre sus estructuras. Se deberá ser hábil para dominar el espacio de batalla y controlar el ambiente de información; empleando equipos que envuelven el uso de tecnologías comerciales y militares disponibles en el país, que satisfagan las necesidades de comunicaciones y distribución de comando y control (C^2), balanceando el desarrollo tecnológico con un menor costo para el ejército dentro de las exigencias de seguridad y fines por alcanzar.
g. Una concepción moderna del apoyo de Telemática deberá visar ganar la guerra de información (G-I), empleando recursos apropiadamente sincronizados e integrados con otros institutos y dependencias gubernamentales o comerciales; que nos posibilite de manera efectiva ser hábiles para capitalizar dentro del ambiente de la información, al mismo tiempo que se protege las posibilidades de información amiga de la explotación enemiga; negándosele o retringiéndosele el uso de dicho ambiente para el C^2 de sus fuerzas y actividades. Para ello deberemos

contar y saber emplear equipos fijos, móviles, guiados electrónicamente; o, tripular y operar eficientemente equipamiento sofisticado para alcanzar la sincronización e integración del C^2 de los diversos elementos del combate.

h. Para ganar la G-I, el apoyo de Telemática ha sido y siempre será un factor importante; sin embargo hoy más que antes un comandante debe tener "información esencial" disponible de todas las partes de su espacio de batalla para tener éxito; y, esto será dependiente de la disponibilidad de comunicaciones horizontal y verticalmente establecidas con todos los elementos con que necesita enlazarse, con paquetes de comunicaciones altamente móviles y versátiles; y que dentro de las limitaciones económicas y presupuestarias se acerquen lo más posible a la tecnología del estado del arte.

i. El ejército en la era de la información y la tecnología dependerá de la inteligencia y ésta del apoyo de Telemática, para contar con información en tiempo real o en tiempo casi real en los niveles estratégico, operacional y táctico. Pero la inteligencia es sólo una de las áreas funcionales de un campo de batalla moderno o también llamados sistemas operacionales del campo de batalla (SOC´s), pues también existen las áreas de: maniobra, apoyo de fuegos, defensa aérea, comando de batalla, guerra electrónica, movilidad y supervivencia y apoyo administrativo. Todas estas áreas poco a poco irán empleando tecnologías automatizadas que deberán ser apoyadas con sistemas automatizados del campo de batalla (SAC´s), que consisten de hardware y software de computadoras que organizan y manejan la información del campo de batalla que los comandantes (cmdtes) y sus estados mayores (EEMM) necesitan. Esta información será presentada en varias formas o categorías: voz, mensajes gráficos o escritos, datos de computadoras (máquina a máquina) e imágenes.

j. Toda esta carga de información deberá colocarse y pasarse sobre infraestructuras de sistemas de información automatizados (SIA´s) y redes de telecomunicaciones; lo cual pone al apoyo de Telemática como el objetivo principal por atacar, destruir, degradar y/o dislocar. Los nuevos avances tecnológicos están cambiando la manera de conducir las operaciones (opns) militares en todos los niveles de la guerra, convirtiendo al apoyo de Telemática en un multiplicador de la fuerza con el énfasis orientado a ganar la G-I.

k. Otro concepto fundamental del apoyo de Telemática hoy en día, es que la naturaleza de las guerras modernas está en que es conjunta en esencia y en muchos casos llegará a ser multinacional o combinada, colocando nuevos retos para diseñar redes de comunicaciones no sólo para apoyar a las fuerzas (fzas) del ejército sino también con capacidad para integrarse y enlazarse con otros institutos y organizaciones civiles, lo que trae y añade complejidad para la interoperatividad de las comunicaciones.

l. Finalmente, los comunicantes debemos recordar que aún en la era de la información, la guerra continuará siendo un esfuerzo de dimensión humana, sujeta a emociones y caracterizada porque habrá derramamiento de sangre. De ahí que los cmdtes buscarán minimizar los riesgos de pérdidas de vidas, conforme el avance tecnológico vuelva más letales y precisas a las armas, dispersando a las tropas y unidades; complicando aún más el apoyo de Telemática para mantener el C^2.

04. EL AMBIENTE ELECTROMAGNETICO Y EL APOYO DE TELEMÁTICA

a. La importancia del ambiente electromagnético en la guerra moderna está ampliamente explicado en el manual de doctrina general de guerra electrónica (Ed 1998). Como se detalla en dicho manual, el ejército en una guerra del siglo XXI deberá combatir para obtener victorias y estar preparado para ganar la primera batalla, contra cualquier amenaza, en cualquier lugar y con el máximo de nuestra potencia combativa concentrada en el momento decisivo. Se debe asumir que es muy probable que el adversario que enfrentemos posea posibilidades tan efectivas como las nuestras y quizás con mayor cantidad de recursos que los que podamos desplegar, por lo menos en las etapas iniciales del conflicto.

b. El ganar la primera batalla será crítico, ya que puede ser también la última, debido a la letalidad de las armas modernas, a su precisión destructiva y a la globalización e internacionalización de los conflictos, que rápidamente pueden influir en la detención de la guerra con una de las partes en mejor posición negociadora que la otra.

c. Para ganar la primera batalla, los cmdtes del comando de batalla deben tener información relevante e inteligencia (IRI) que les permita el C^2 de sus fzas. La respuesta a este requerimiento es el apoyo de Telemática y este apoyo sólo es posible en el ambiente electromagnético, para que sea rápido, preciso y en cualquier lugar y momento que se desee. En este ambiente electromagnético se producen las comunicaciones, se establecen los enlaces a distancias, se da el flujo de informaciones, pero también está lleno de retos y amenazas mediante la guerra electrónica (GE). Se produce así en este ambiente un combate invisible, pero tan letal como cualquier arma de apoyo de fuego convencional; este combate se libra para obtener la superioridad o dominio del espectro y de la información que fluya por él. Por lo tanto el apoyo de Telemática deberá darse no sólo para asegurar la continuidad de los enlaces, sino para protegerlo contra los intentos adversarios por degradarlos y destruirlos.

05. EL COMANDO Y CONTROL Y EL APOYO DE TELEMÁTICA

a. El comando y control (C^2) es un elemento esencial del arte y ciencia de la guerra. Es el ejercicio de la autoridad y dirección de un cmdte sobre las fuerzas puestas bajo su mando para el cumplimiento de su misión; cuyas funciones son realizadas a través de un arreglo de personal, equipos, comunicaciones, facilidades y procedimientos que un cmdte emplea para planear, dirigir, coordinar y controlar sus fzas y opns.

b. El centro de C^2 es el cmdte, quien emplea a su EM y a sus comunicaciones como sus recursos más importantes para ejercer ese C^2, de ahí que a las comunicaciones se le conoce como el arma del comando. El C^2 es una entidad unificada, ya que el cmdte no puede comandar efectivamente sin control, y él no puede ejercer el control sin comandar. El objetivo del C^2 es el cumplimiento de la misión, mientras que el objeto del C^2 son las fuerzas.

c. Para ejercer un efectivo C^2, el cmdte deberá poseer un eficiente sistema de apoyo de Telemática que responda de manera inmediata a sus necesidades críticas de información (NICC: necesidades de información crítica del cmdte) y que les permita conducir, dirigir y/o controlar sus fuerzas y operaciones. Este sistema de apoyo de Telemática está básicamente compuesto por un miembro de su EM de coordinación, el G-

6/S-6 (Oficial de operaciones de Telemática) quien planea, aprecia, recomienda y en algunos casos comanda, el empleo de organizaciones de comunicaciones en cada escalón de comando, que constituye el otro gran elemento del sistema de apoyo de Telemática.

d. Los cmdtes y sus comunicaciones, son hoy en día entidades inseparables, serán los primeros objetivos a destruir por las fuerzas adversarias; de ahí que las comunicaciones siguen siendo una responsabilidad del comando en todos los escalones y requerirán que ellos digan a sus G-6´s / S-6´s algo más que simplemente "cuide de ellas".

e. El sistema de comando y control

(1) El sistema de C^2 está definido como las instalaciones, equipamiento, comunicaciones, procedimientos y personal esencial para que un cmdte planee, dirija y controle las opns de sus fzas asignadas en el logro del cumplimiento de su misión.

(2) El sistema de C^2 es una organización de recursos que el comandante emplea para ayudarlo a planear, dirigir, coordinar y controlar las operaciones militares para asegurar el cumplimiento de su misión. El resultado es la eficiencia combativa. Los recursos que el comandante y su unidad necesitan para realizar las funciones críticas de comando y control incluyen:

(a) Personal, (el EM y personal de enlace), quienes ayudan al Comandante en el ejercicio del control.

(b) Comunicaciones, que incluyen equipamiento terrestre y satelital, y las redes.

(c) Equipamiento, tal como equipos de automatización (computadoras) para proyectar las actividades de C^2; y, los materiales para sostener los recursos dedicados para el apoyo al C^2.

(d) Instalaciones, que incluyen ambientes de trabajo seguros o Cuarteles Generales (Puestos de Comando) para el Comandante y su EM.

(e) Facilidades administrativas y de seguridad, que incluye elementos u organizaciones encargadas de proteger, mantener y mover al Comandante y su EM.

(f) Procedimiento (incluye aquellos para el proceso de toma de decisiones), empleando múltiples fuentes tales como doctrina vigente, tácticas, técnicas, regulaciones, reglamentos, procedimientos operativos estandarizados; orientados al esfuerzo del Cmdte y del EM.

(3) El sistema de C^2 debe ser flexible, robusto, con capacidad de supervivencia y capaz de proveer al Comandante con información que le permita realizar las funciones de C^2 de manera concurrente. El comandante es el centro alrededor del cual el sistema de C^2 gira. Cualquier área donde las funciones se superponen, señalará normalmente donde él debe enfocar su atención personal. El EM, emplea el sistema C^2 para proporcionar al Comandante la libertad necesaria para enfocarse sobre el área que él ha considerado como la más importante.

(4) Ni el comandante ni su EM deberían considerar al sistema de C^2 como un fin en sí mismo. El sistema sólo existe para apoyar al comandante y ayudarlo en su toma de decisiones necesarias para el cumplimiento de su misión. Por ejemplo, mientras está ejercitando su comando, un

comandante emite órdenes que sirven como entrada a las Unidades subordinadas. Conforme cada Unidad subordinada planea y ejecuta su misión, se produce retroalimentación para su comandante inmediato superior y su EM. Estas son las medidas esenciales que soportan a un efectivo C^2. El Comando y Control es continuo y sus actividades están interrelacionadas.

SECCION II. FUNDAMENTOS DEL APOYO DE TELEMÁTICA

06. MISION GENERAL DEL APOYO DE TELEMÁTICA

a. Bajo un concepto moderno, la misión general del apoyo de Telemática es proporcionar apoyo de combate a los cmdtes de todos los escalones y en todos los niveles de la guerra, con los medios que le permitan el comando y control sobre el campo de batalla en todo el rango de las operaciones militares.

b. La misión del apoyo de Telemática se materializa proporcionando redes colectivas, integradas y sincronizadas, así como sistemas de información (SINFOR) para apoyar a las capacidades del combate a través de todo el rango de las opns militares; proveyendo al cmdte los medios que le permitan comunicar su intención y el C^2 de sus fzas, asegurando la superioridad del ciclo de decisión. Sin el apoyo de Telemática, será imposible para los cmdtes alcanzar sus objetivos y conducir exitosamente sus campañas, sus opns mayores, sus batallas y combates tácticos; y una guerra total.

c. El apoyo de Telemática engloba todos los procesos para mover la información mediante el empleo de todos los medios disponibles de trasmisión y de reunión de info. Este apoyo debe ser lo suficientemente flexible para extenderse desde el nivel estratégico hasta el nivel táctico más bajo, haciendo que la info esté disponible cuando y donde se le necesite sin restricciones artificiales.

d. El objetivo que visa la misión general del apoyo de Telemática es proporcionar una arquitectura de apoyo de comunicaciones casi perfecta que sea segura, confiable, flexible y compatible con la mixtura de fuerzas e institutos apoyados, de apoyo y adyacentes. Esta arquitectura debe hacer que los numerosos elementos distribuidos en un campo de batalla se relacionen en una red integrada, interoperable y cohesiva, dentro de las capacidades de la infraestructura de comando, control, comunicaciones, computación e inteligencia (C^4 I).

e. La rápida proliferación de la tecnología de comunicaciones comerciales hace imperativo que el ejército permanezca atento a los cambios del ambiente de información global (AIG); para lo cual el G-6/S-6 y los cmdtes de las unidades de comunicaciones deben asegurarse que las comunicaciones que proporcionen al combatiente estén protegidas y sean confiables. La info que se recibe con exactitud y a tiempo (oportunamente) puede incrementar grandemente el tiempo disponible para la toma de decisión por un cmdte, así como ayudarlo en el entendimiento total del estado de su misión en los puntos cruciales en el ciclo o proceso de toma de decisión.

f. Muchos cmdtes tácticos participarán en el apoyo de Telemática, cuando ellos mismos operan o administran sus sistemas de información funcional

que conectan a los sistemas y redes de comunicaciones, que les permita dirigir, coordinar y apoyar a las fuerzas de combate, de apoyo de combate y de apoyo administrativo

g. Este apoyo de Telemática abarca una serie de disciplinas que administran la información denominadas:
   (1) Operaciones de Comunicaciones
   (2) Administración de la automatización
   (3) Seguridad de la información (o de Telemática)
   (4) Información Visual (IV)
   (5) Guerra Electrónica
   (6) Diversos (particularmente la administración de los servicios de información del campo de batalla)

h. Las responsabilidades y funciones del apoyo de Telemática en cada una de estas disciplinas varía con los niveles de la guerra (táctico, operacional y estratégico) y será tratado con mayor detalle en párrafos, secciones y capítulos posteriores.

07. TAREAS ESENCIALES DEL APOYO DE TELEMÁTICA

a. El apoyo de Telemática a una fuerza combatiente demanda el cumplimiento de una serie de tareas, derivadas de la misión general y del propio proceso del planeamiento militar para tomar decisiones (PMTD) (Ver ME 11-30, ed. 1999). Estas tareas pueden formar parte de los procedimientos operativos vigentes (POV´s) del Comando respectivo, siempre y cuando hallan sido debidamente entrenadas y si las tropas y personal de comunicaciones son conscientes de los principios de apoyo de Telemática (ver párrafo 08).

b. A continuación se describen algunas tareas esenciales:

Integrar el C^2 de la fuerza en todos los escalones.- El apoyo de Telemática debe integrar todos los sistemas de información empleados por los elementos del campo de batalla para apoyar el C^2 del combatiente. La estructura del apoyo de Telemática proporciona los medios para obtener, distribuir y almacenar la información con oportunidad, precisión y confiabilidad en todos los escalones. Esta información va y viene en los escalones de cmdo de la fuerza y sus EEMM, asi como entre áreas funcionales y EEMM.

Apoyar al P/O u O/O hasta el P/Batalla.- El apoyo de Telemática debe maximizar la efectividad del combate desde el teatro de la guerra hasta el nivel Compañía y aún hasta los equipos de combate. Las operaciones en el campo de batalla se retrasmiten sobre el apoyo de Telemática para sostener el plan de batalla. Los procesadores de datos, los equipos de telecomunicaciones y los servicios de información del campo de batalla proveen información para las necesidades críticas, que permitan al Cmdte explotar las oportunidades.

Sincronizar las operaciones de la fuerza.- Significa que los medios de comunicaciones se enfoquen sobre la máxima potencia combativa en el punto decisivo para derrotar al enemigo. El éxito de la operaciones ofensivas depende de la habilidad de las fuerzas amigas para encerrar al enemigo y destruir su voluntad de lucha. La sincronización será importante para las operaciones del ejército, aunque puede ser más difícil cumplirlo. El apoyo de Telemática proporciona al Cmdt los medios para sincronizar las operaciones de la fuerza.

Sostener las operaciones de la fuerza.- El apoyo de Telemática asiste en la provisión de medios para obtener, procesar, proyectar, almacenar y distribuir información para apoyar a las operaciones de toda la fuerza de manera contínua y sostenida.

08. PRINCIPIOS DEL APOYO DE TELEMÁTICA

a. Los principios de apoyo de Telemática son cuatro: continuidad, seguridad, versatilidad y simplicidad. Estos principios apoyan el flujo de información entre los elementos de la fuerza sin importar la función, arma, servicio o instituto. Seguir y respetar estos principios asegurará que el apoyo de Telemática sea sistemático y consistente en el desarrollo de las redes. Adicionalmente estos principios promueven un efectivo comando y control así como el apoyo a otros elementos combatientes. Estos principios se aplican tanto a los EEMM funcionales, EEMM de unidades de comunicaciones y combatientes o usuarios involucrados con las operaciones de Telemática.

b. Continuidad

(1) Es la disponibilidad ininterrumpida de los enlaces y flujos de información, así como la implementación de plataformas efectivas de comando y control. En situaciones de combate, el Cmdte y su EM deben tener información actual y precisa, que les permita ejercer o ejecutar sus deseos, concentrar sus recursos disponibles y sincronizar sus dispersas actividades de apoyo.

(2) La continuidad afecta la habilidad de los combatientes para visualizar el campo de batalla, ejercer la iniciativa, sincronizar los efectos, lograr agilidad y explotar los éxitos.

(3) Con la continuidad, el combatiente puede aumentar el espacio para la maniobra y agregar profundidad a las operaciones de combate. Puede también emplear sistemas de armas más complejos y letales, así como puestos de comando dispersos y altamente móviles.

(4) Finalmente con la continuidad, el Cmdte puede degradar la habilidad enemiga para desorganizar nuestros sistemas de apoyo de Telemática.

(5) La continuidad requiere que los elementos subordinados apliquen: la supervivencia, la confiabilidad, la redundancia y la conectividad:

(a) Supervivencia.- Es la habilidad para operar después de una pérdida de combate. Es el proceso de sostener, sin pérdidas, el flujo de información desde y hacia el combatiente, lo que demandará que como mínimo los medios de apoyo de Telemática estén siempre disponibles. Las redes de comunicaciones robustas, empleando principios sensatos de salto de frecuencia, rutas alternas y equipos de reserva, asegurarán la supervivencia. La dispersión física de las unidades, medidas de protección electrónica y aumento de la movilidad de los equipos mejorarán la supervivencia.

(b) Confiabilidad.- Está dada por el empleo de procedimientos apropiados de apoyo de Telemática, equipos bien mantenidos y operadores bien entrenados. La confiabilidad permitirá que el combatiente tenga información completa, precisa y actual que le

permita tomar decisiones informado y lograr el máximo potencial de combate.

(c) Redundancia.- Significa duplicar medios y proporcionar enlaces alternos para el flujo de información, de tal manera que la información crítica siempre esté disponible cuando y donde se necesite. Las redes ganan redundancia mediante la provisión de sistemas automáticos, enrutamiento en tiempo real y por tener la capacidad para una rápida reconstitución y reorganización.

(d) Conectividad.- Son enlaces de información y comunicación establecidas de acuerdo a las normas de comunicaciones (superior al subordinado, de izquierda a derecha, la que refuerza a la reforzada, la que apoya a la apoyada). La conectividad asegura el comando y control de las fuerzas que están dispersas y operando en un ambiente móvil.

c. Seguridad

(1) La seguridad ayuda a mantener la integridad de la fuerza; y se aplican a: la seguridad de los sistemas de información, seguridad física, dispersión y al engaño.

(2) Seguridad de los sistemas de información.- Son procedimientos que reducen la posibilidad que personas no autorizadas obtengan información desde los sistemas de apoyo de Telemática. Estos procedimientos abarcan los principios de la Seguridad de Telemática (SEGELEC: Seguridad Electrónica y SEGCOM: Seguridad de Comunicaciones) y de la Seguridad Física. Los virus destructivos y bombas lógicas insertadas o introducidas en el software pueden causar sabotaje de la red entera y pérdida de información crítica. Los componentes críticos de la seguridad de los sistemas de información que deben emplearse son: protección del password, detección del intruso y herramientas de escaneo de virus.

(3) Seguridad Física.- Es la protección del equipo y lugares físicos contra el ataque o detección enemiga. Las técnicas de seguridad física limitan la habilidad enemiga para obtener peculiaridades visuales, acústicas, térmicas o electrónicas de los sistemas amigos.

(4) Dispersión.- Es la separación geográfica de las fuerzas sobre el campo de batalla. La dispersión aumenta la flexibilidad y optimiza la supervivencia para las tropas y para los recursos de C^3I (Comando, Control, Comunicaciones e Inteligencia).

(5) Engaño.- Particularmente el engaño electrónico, es la alteración deliberada de Telemática similares que apoyan a los nodos en las múltiples ubicaciones del campo de batalla. Todo lo referente al engaño electrónico se encuentran en los manuales de guerra electrónica.

d. Versatilidad

(1) Es la habilidad para adaptarse rápidamente a las necesidades de comando y control no previstas, para lo cual deberá existir una arquitectura de información muy bien diseñada, que elimine los límites artificiales que algunas veces existen sobre un campo de batalla.

(2) La versatilidad demanda que el apoyo de comunicaciones sea flexible, móvil y adaptable a todas las posibles condiciones del campo de

batalla; permitiendo la conexión entre fuerzas conjuntas para el apoyo mutuo.

(3) Los componentes de la versatilidad son: flexibilidad, interoperatividad y autonomía:

(a) Flexibilidad.- Es el apoyo a las fuerzas de maniobra que requiere movilidad física, velocidad y flexibilidad electrónica; para que el apoyo de Telemática facilite la ventaja posicional, la sorpresa y la habilidad para concentrar las fuerzas decisivamente. Esto se logra proporcionando una red de C^2 robusta. La flexibilidad electrónica es la habilidad para expander, contraer o cambiar los sistemas de apoyo de Telemática conforme la situación lo imponga. A nivel táctico, las fuerzas pueden intercambiar información sin reconfigurar las redes de comunicaciones; pero a nivel estratégico – operativo deberán dispersarse y diversificarse los recursos de comunicaciones.

(b) Interoperatividad.- Es la posibilidad de poder intercambiar información y servicios de telecomunicaciones, directa y satisfactoriamente entre usuarios. Esto será crítico en la guerra moderna, donde las fuerzas conjuntas serán los actores principales en los conflictos. La interoperatividad del apoyo de Telemática requiere de procedimientos, sistemas y equipos de C^3 compatibles. La interoperatividad será mejorada mediante las acciones siguientes:

1. Definiendo protocolos y parámetros de interface específicos entre todas las redes y sistemas potencialmente enmallados.
2. Desarrollando tácticas, técnicas y procedimientos (TTP) comunes.
3. Incrementando los procedimientos de interoperatividad de apoyo de Telemática inter e intra – institutos (coordinación de frecuencias, IOCE, acuerdos de estandarización, protocolos de estandarización, elementos o datos comunes y/o diccionarios conjuntos).
4. Estableciendo programas de entrenamiento conjunto de comunicaciones.
5. Proporcionando apreciaciones de apoyo de comunicaciones y contínua actualización de informaciones.
6. Identificando y preparando recursos para contingencias.
7. Planeando requerimientos de C^2 no esperados.

(c) Autonomía.- Es la habilidad de un Cmdte local para realizar sus tareas de manera independiente, para lo cual se requiere descentralizar la delegación de autoridad, responsabilidad y recursos de C^2 al Cmdte subordinado y que éste entienda la misión e intención del cuartel general superior y ejercite su iniciativa. Un apoyo de Telemática óptimo permitirá a los Cmdtes ubicarse donde quiera que ellos lo deseen, de tal manera de ser capaces de ejercitar el C^2 de sus fuerzas en todo momento; a su vez el EM también deberá ser capaz de llevar a cabo la operación planeada con o sin la presencia de su Cmdte.

e. Simplicidad
   (1) La simplicidad resulta cuando los Cmdtes, el EM y las tropas usan y mantienen los recursos de apoyo de Telemática; lo que tendrá un profundo efecto sobre la conducción y eficiencia de todas las operaciones militares.
   (2) Los sistemas C^2 automatizados deben ser simples de instalar, operar y mantener por todos los integrantes de la fuerza debidamente entrenados. Consta de dos elementos: sofisticación tecnológica y estandarización. La sofisticación tecnológica provee sistemas de comunicaciones efectivos, confiables y de fácil mantenimiento; maximizando el procesamiento y obtención de información, pero también requiere de entrenamiento integrado y mejorado de los operadores. La estandarización asegura que los sistemas de apoyo de Telemática de las fuerzas tácticas, operacionales y estratégicas, cuenten con compatibilidad física y electrónica; facilitando un método y medio uniforme para integrar la información y transferencia de C^2; a la vez que simplifica la sincronización y control de todas las fuerzas.

09. REDES Y SISTEMAS DEL APOYO DE TELEMÁTICA

a. Una red es un conjunto de componentes o subsistemas de conmutación y trasmisión enlazados como un todo. Esto incluye todos los componentes de hardware y software de comunicaciones construidos/instalados en los subsistemas de conmutación y trasmisión; y, las comunicaciones relativas a los componentes de hardware y software construidos/instalados en los receptores, en las facilidades, así como en la existencia de personal especialista en la operación y de procedimientos que apoyen los requerimientos operacionales.
b. Un sistema es recursos de información y procesamiento de datos, asociado a aparatos periféricos, aplicaciones de soporte e infraestructura de red de comunicaciones de sistema abierto que interconecta a los usuarios finales y los componentes del sistema. Los sistemas incluyen a los receptores (hosts), sistemas operativos, periféricos, aplicaciones de sistemas finales, base de datos y archivos; así como el hardware y software, facilidades, personal y procedimientos necesarios para apoyar las aplicaciones y requerimiento operacionales.
c. La administración de redes y sistemas (ARS) es un conjunto de actividades, tareas, capacidades y herramientas que se requieren para establecer una red o sistema, mantenerlo operando, optimizar su rendimiento, mantener los cargos para su uso y proteger los servicios que provee. La administración de redes y sistemas comprende:
   (1) Planeamiento
   (2) Ingeniería de redes y sistemas
   (3) Provisión de servicios
   (4) Medidas de servicios
   (5) Administración
   (6) Logística
   (7) Areas funcionales de administración específica (AFAE):
      (a) Administración de fallas/desperfectos de la red o sistema.
      (b) Administración del rendimiento de la red o sistema.
      (c) Administración de la configuración de la red y/o sistema.
      (d) Administración de la seguridad de la red y/o sistema.

(e) Administración de los cargos.

d. La ARS posibilitará que los cmdtes y EEMM de las organizaciones y elementos de comunicaciones, entiendan mejor como llevar a cabo sus objetivos en apoyo a las misiones operacionales del ejército, distribuyendo sus escasos recursos de personal y tecnológicos más rápido, más económica y eficientemente en apoyo directo a la fuerza que se despliegue. Por otro lado, los procedimientos y herramientas de administración de redes automáticas reducirán los costos y requerimientos de entrenamiento al mismo tiempo que mejorarán la habilidad para intercambiar información relevante. Esto demandará la aplicación de estándares comúnmente aceptados en la compra de herramientas de software y en el empleo de productos terminados comerciales y estatales siempre que sea posible.

e. El apoyo de Telemática se realiza básicamente a través del establecimiento de redes y/o sistemas que integran las comunicaciones y los sistemas de información (SINFOR). Esta integración se realiza mediante el establecimiento de la arquitectura de información del campo de batalla que considera a: las redes de área local (LAN´s), redes de área amplia o global (WAN´s) y sistemas de información automatizados (SIA); que posibilite a los cmdtes en todos los escalones, el C^2 de sus fzas. El establecimiento de la arquitectura de info del campo de batalla, se basa en el concepto de administración de la info del área que incluye recursos y actividades empleados en la obtención (adquisición), desarrollo, procesamiento, trasmisión, distribución, recuperación, mantenimiento, disposición y manejo de la info en un área y a través de todos los niveles de la guerra. Estos recursos de info consideran la doctrina, políticas, datos, equipamiento, personal, servicios, instalaciones y unidades de comunicaciones. A continuación se describen brevemente las redes y sistemas básicos:

(1) Redes de área local (LAN: Local Area Networks)

(a) Son computadoras enlazadas en conjunto mediante medios de trasmisión físico (cable, alambre o fibra óptica), que permiten compartir la información entre dichas computadoras enlazadas y otras computadoras de otras LAN´s. La interconexión de redes de área local pueden conformar una red de área amplia o global (WAN). Las salidas o puentes (“gateways”) o enrutadores (“routers”) permiten dicha interconexión. Un gateway es una combinación de hardware y software que permite a los usuarios de una red accesar a los recursos en un diferente tipo de red.

(b) Dentro de la nueva concepción del apoyo de Telemática a las operaciones militares, el gateway o puerto para una LAN táctica estará en el centro de operaciones táctica (COT) de una DE o EO (Ver Cap 7 Secc III del ME 11-30, Organización y Opns de EM de Comunicaciones, ed 1999); o en los nodos de pequeña extensión (NPE) de una unidad de comunicaciones (conocidos antes como centros de comunicaciones) que apoyan a un puesto de comando hasta el nivel Gran Unidad.

(c) El G-6/S-6 establecerá la conectividad al nodo de pequeña extensión cuando el puerto (gateway) está en el NPE de la Unidad de Comunicaciones que apoya. Cuando el puerto está dentro de un COT, el G-6 del EO/DE dispondrá que la Unidad de comunicaciones que apoya a dicha fza establezca la

conectividad al puerto. Tanto el cmdte de la unidad de comunicaciones que apoya, como el G-6/S-6 de la unidad apoyada, configurarán, operarán y mantendrán la conectividad a una WAN cuando sea requerido.

(d) Para las unidades de combate, apoyo de combate y apoyo administrativo, dentro del concepto de apoyo de Telemática con LAN´s; se ha desarrollado el concepto de redes de radio monocanal de combate (CNR: Combat net radio) como internet táctica; que conjuntamente con las redes de equipos terminales móviles de usuarios para niveles GU y superiores (redes WAN); constituirán el soporte o "back bone" de la arquitectura de comunicaciones para las posibilidades o capacidades de voz, datos y algo de imagen (vídeo lento, videoconferencia o imagen congelada).

(e) Todas estas redes tendrán también herramientas de planeamiento que permitan al administrador de la red (G-6/S-6) lo siguiente:

1. Planear, diseñar y/o diagramar la red.
2. Realizar el modelado a través del análisis de carga de comunicación.
3. Probar la configuración de la red y del sistema.
4. Distribuir electrónicamente la configuración de los usuarios y otra información de base de datos, cuando se inicialize y actualice.

(f) Mayor información sobre los aspectos tratados en este subpárrafo, será vista a través del desarrollo de este manual y otros manuales más específicos como el manual de administración de redes y sistemas y el manual de internet táctica, ambos en producción en la Escuela de Comunicaciones.

(2) Redes de área amplia / global (WAN: Wide Area Network)

(a) Estas redes son recursos de comunicaciones enlazados en conjuntos por sistemas sobre áreas dispersos. Una WAN puede ser dos o más LAN´s dispersas geográficamente pero conectadas con un enlace común.

(b) Las WAN´s pueden hacerse con recursos estratégicos, operacionales y/o tácticos. Ejemplos de arquitecturas WAN´s lo constituirán: los sistemas de comunicaciones de área de usuario común (niveles DE/EO y TO), sistema de redes de equipos terminales móviles de usuarios (niveles GU y superiores), sistema de redes de radio monocanal de combate (integración de redes de unidades tipo batallón y menores de una misma organización o GU/EO), sistema de distribución de datos y sistemas de comunicaciones de radiodifusión sonora y/o televisiva y datos de navegación / posicionamiento. La internet táctica también es considerada como una red WAN.

(3) Sistemas de Información Automatizados (SIA)

Son cualquier ensamblaje o reunión de hardware, software o firmware de computador; configurado para colectar/ reunir, crear, comunicar, computar, difundir, procesar, almacenar o controlar datos o información en una forma electrónica. Estos SIA´s incluyen computadoras independientes o autónomas, pequeñas computadoras

o computadoras personales (PC´s), procesadores de palabras, computadoras de multiusuarios, terminales y redes.

10. LOS PRINCIPIOS DE LA GUERRA Y EL APOYO DE TELEMÁTICA

a. Durante los últimos 200 años, la guerra ha sido llevada a cabo por cmdtes versados (en grados variables) en los (09) principios de la guerra siguientes: objetivo, ofensiva, masa, maniobra, economía de fuerzas o medios, unidad de comando, seguridad, sorpresa y simplicidad. Los subpárrafos siguientes describen como el apoyo de Telemática fusiona, combina, define, crea y apoya estos principios en un campo de batalla moderno.

b. Objetivo: "Dirigir las opns militares hacia un objetivo claramente definido, decisivo y alcanzable". El planeamiento del apoyo de Telemática debe incluir este principio. Los objetivos del cmdte de la fza son convertidos en misiones y prioridades a las unidades de maniobra, de apoyo de combate y apoyo administrativo. Estas misiones y prioridades deberán estar claramente definidos y ser alcanzables.

c. Ofensiva: "Alcanzar, retener y explotar la iniciativa". Los cmdtes quienes reconocen y alcancen una situación favorable se crearán oportunidades para la victoria en la batalla. El apoyo de Telemática deberá siempre ser proporcionado dentro del espíritu de la ofensiva. La maniobra de la fuerza apoyada requerirá del empleo de los medios de apoyo de Telemática para mantener la movilidad de esa fuerza.

d. Masa: "Concentrar la potencia combativa en el lugar y tiempo decisivo". El apoyo de Telemática provendrá de múltiples sistemas de información (SINFOR), dispersados en todo el campo de batalla, mejorando la habilidad del cmdte para concentrar sus recursos.

e. Maniobra: "Colocar al enemigo en una posición de desventaja mediante el uso flexible de la potencia combativa". Para el apoyo de Telemática, significará su habilidad para desplegarse y desplazarse rápidamente para mantenerse a la par con la fuerza que maniobra.

f. Economía de medios o fzas: "Distribuir la mínima y esencial potencia combativa para los esfuerzos secundarios". El apoyo de Telemática debe cumplir con este principio asignando a la misión dada los recursos y esfuerzos que no excedan lo necesario para producir o alcanzar el objetivo deseado, en particular si aún existieran otras misiones o tareas por apoyar.

g. Unidad de Comando: "Para cada objetivo, asegurar la Unidad de esfuerzo bajo un cmdte responsable". El apoyo de Telemática deberá asegurar la sincronización sobre el campo de batalla, poniendo a disposición del cmdte de la fza los recursos que le permitan lograr la unidad de comando de una manera transparente. Para lo cual las relaciones de comando y de apoyo de Telemática deberán estar bien definidas para permitir que los recursos de apoyo de Telemática sean consistentes con la situación táctica u operacional. El G-6/S-6 de cada escalón proporcionará la misma consistencia para todas las operaciones.

h. Seguridad: "No permitir nunca que el enemigo gane una ventaja inesperada". Durante las opns militares deberán tomarse las medidas de seguridad tácticas. Hay dos aspectos de la seguridad que se relacionan con el apoyo de Telemática: el primero se refiere a que la importancia de proporcionar apoyo continuo de comunicaciones no puede poner en peligro la seguridad de la fuerza o si lo hace, será después de haberse calculado los riesgos; y el segundo aspecto envuelve la seguridad física de los

recursos de apoyo de Telemática como por ejemplo los nodos de conmutación, que son objetivos de alto costo para la fuerza enemiga. Estos recursos necesitarán protección.

i. Sorpresa: "Golpear al enemigo en el momento, lugar o circunstancia para la cual no estaba preparado". La sorpresa permite ganar la iniciativa, amenazar la moral del adversario y reducir las bajas de nuestras fzas. El apoyo de Telemática para alcanzar la sorpresa se realizará proporcionando continuidad a todas las etapas de una opn (planeamiento, emisión de órdenes y ejecución), participando en los planes de engaño y seguridad de las opns (SEGOPE).

j. Simplicidad: "Preparar planes y órdenes claras, concisas y simples que aseguren un entendimiento total". La velocidad de los eventos, la complejidad de la guerra moderna y las situaciones cambiantes del medio ambiente; pueden ocasionar considerable confusión. El apoyo de Telemática proporcionando conectividad, continuidad, uniformidad e interoperatividad en las opns estrechas, profundas y en retaguardia, permitirán innovar la coordinación intensiva y administración de los medios reduciendo los riesgos de confusión y caos. De ahí que los planes y órdenes de comunicaciones deberán ser simples, claros y concisos para reducir la confusión y asegurar el éxito.

11. NORMAS GENERALES DEL APOYO DE TELEMÁTICA

a. Las normas generales del apoyo de Telemática, anteriormente llamadas normas de comunicaciones, no han variado a pesar que el adelanto tecnológico en los equipos y sistemas de información; permiten fácilmente establecer enlaces en todas las direcciones, particularmente se ha posibilitado los enlaces horizontales y la redundancia de los mismos para asegurar la continuidad como un principio de apoyo de Telemática.

b. Esta normas que aún permanecen invariables, se basan en los principios del enlace (Ver Anexo 06, el enlace; del ME 11-30, organización y opns de EM de comunicaciones; párrafo 04) y son las siguientes:
   (1) La unidad del más alto escalón establece enlace con las unidades subordinadas.
   (2) La unidad que apoya (con fuegos, GE, ingeniería, etc) establece enlace con la unidad apoyada.
   (3) Los enlaces laterales se establecerán según lo dispuesto por el escalón superior, a falta de instrucciones específicas, la unidad de la izquierda establecerá enlace con la de su derecha.
   (4) Las del mismo escalón y unidades de retaguardia establecen enlace con aquellas de adelante.
   (5) Las unidades que no están al contacto con el enemigo establecerán enlace con las que si lo están.
   (6) Cuando se conduzca un pasaje de líneas, la unidad que se mueve establece enlace con la estacionada (en posición), tanto para movimientos hacia delante como hacia retaguardia.
   (7) La fuerza que llega establece enlace con la fuerza que sale durante un relevo de tropas de combate.

c. Existen otras normas que no se relacionan al enlace necesariamente sino al apoyo de Telemática en sí, y son las siguientes:
   (1) La distribución de los medios de comunicaciones no es homogénea, sino adaptada a la situación.

(2) Las necesidades de enlace deben satisfacerse simultáneamente por varios medios de comunicaciones (redundancia).
(3) Los sistemas de comunicaciones en funcionamiento deberán servir de base para apoyar a las opns futuras.

12. LAS OPERACIONES DE INFORMACION Y EL APOYO DE TELEMÁTICA

a. Las operaciones de información (OI) están basadas en la administración y protección de la info amiga; y en la explotación de los sistemas enemigos para lograr una ventaja de la info en opns militares. Es el proceso de proporcionar al combatiente con info y datos relevantes que sean superiores a cualquier oponente mediante la ejecución efectiva de la misión de apoyo de Telemática.
b. El rápido avance en la difusión y empleo de las tecnologías de la info han acelerado el ritmo en el cual los combatientes deben tomar decisiones y han incrementado el impacto de esas decisiones sobre las fuerzas amigas y enemigas en los niveles táctico y estratégico de las opns y de la guerra. Las decisiones que algunas veces no eran conocidas en los escalones más bajos por períodos de días y hasta semanas, ahora llegan a ser relevantes en los niveles tácticos en algunos segundos. Los cmdtes y sus EEMM deben conocer y entender como administrar las OI en este nuevo escenario, ya que demasiada información puede probar ser tan "mortífera" como información insuficiente; por lo tanto la clave será la difusión de sólo información relevante a cada nivel de la opn para ayudar a prevenir la confusión y la sobrecarga de las redes y sistemas.
c. Los cmdtes confían en la info para conducir opns militares exitosas, empleando a los sistemas de información (SINFOR) que soportan a la red de información del combatiente (Ver Sección II del Cap 7 del ME 11-70, empleo de las comunicaciones satelitales en el ejército y el Cap 5 del ME 11-13, operaciones de información). Estos SINFOR están categorizados de la manera siguiente:
   (1) Sistema global de comando y control (SG-C^2)
   (2) Sistema global de apoyo de combate (SG-AC)
   (3) Sistema de comando de batalla del ejército (SCBE), que incluye:
      (a) Sistema de C^2 global del ejército.
      (b) Sistema de C^2 táctico del ejército.
   (4) Sistema de administración de info estándar.
   (5) Sistema de mensajería de defensa.
d. En este manual se tratará con mayor amplitud al sistema de C^2 táctico del ejército (SC^2T), los demás sistemas son de naturaleza estratégica y conjunta y serán desarrollados en manuales especiales.
e. La tecnología actual ha complicado el trabajo de los cmdtes de formas significativas, pero también le permitirá obtener más fácilmente su conciencia situacional del espacio de batalla, permitiéndole incrementar su énfasis en la observación, detección y conciencia total de las actividades de la amenaza o potenciales adversarios. Sin embargo, esos adversarios también pueden obtener información sobre nuestras fuerzas, más aún conociéndose que los aparatos y equipos de procesamiento de info sofisticados están siendo rápidamente accesibles en un mercado comercial abierto a un costo relativamente bajo.
f. Los nuevos sistemas y redes de comunicaciones, que se vienen fabricando y que nuestro ejército está adquiriendo, vienen con microprocesadores y

sistemas operativos incorporados que los pueden hacer vulnerables al ataque de piratas informáticos e intrusos que podrían afectar al apoyo de Telemática en su misión de soportar a la red de información del combatiente. La disciplina de protección de C^2 establece cinco (05) principios para asegurar y proteger la información contra los riesgos y potenciales vulnerabilidades de nuestros SINFOR (Ver párrafo 47 del ME 11-13, operaciones de información).

g. Constituirá un reto para los cmdtes tácticos, los G-6´s / S-6´s y cmdtes de unidades de comunicaciones, proporcionar un apoyo de Telemática continuo, seguro y de alta calidad; mediante la administración de la seguridad de las redes y sistemas que envuelvan aquellas medidas que se toman para mantener un C^2 efectivo de las fzas balanceando las ventajas que le proporciona la digitalización de dichas redes y sistemas, al mismo tiempo que se impide al adversario la posibilidad que nos nieguen info o que influencien, degraden o destruyan nuestros sistemas de C^2.

h. El objetivo de la protección de C^2 será integrar el apoyo de las operaciones de comunicaciones, de la ingeniería técnica, de las disciplinas de seguridad y de la inteligencia (o contrainteligencia); para asegurar la disponibilidad, la integridad y la confidencialidad de la información durante el apoyo de Telemática.

13. DISCIPLINAS QUE ADMINISTRAN LA INFORMACION

a. El apoyo de Telemática en un campo de batalla moderno, abarca mucho más que solo el apoyo de comunicaciones, incluyendo una serie de disciplinas que administran la información de una u otra manera. Estas son:
   (1) Operaciones de comunicaciones
   (2) Administración de la automatización
   (3) Información Visual
   (4) Servicios de Información del Campo de batalla
   (5) Seguridad de la Información
   (6) Guerra Electrónica

b. Las cuatro primeras disciplinas serán desarrolladas en este manual; las otras dos son desarrolladas en el manual de seguridad de comunicaciones y en los Manuales de guerra electrónica, sin embargo en capítulos separados se tratan brevemente.

CAPITULO 2
PRIMERA DISCIPLINA DEL APOYO DE TELEMÁTICA: OPNS DE COMUNICACIONES

SECCIÓN I. INTRODUCCIÓN A LAS OPERACIONES DE COMUNICACIONES

14. CANALES DE FLUJO DE INFORMACION

a. La información operacional normalmente se mueve a través del comando a lo largo de canales específicos. Estos canales ayudan a hacer más eficiente la distribución de la información, asegurando que la información correcta sea pasada de manera oportuna a la persona correcta.

b. Hay tres (03) canales a través de los cuales los comandantes y sus EEMM se comunican: canales de comando, canales de EM y canales técnicos.

(1) Canal de comando.- Es el canal directo que enlaza al Cmdte con sus cmdtes subordinados, o que oficiales de EM autorizados emplean para sus actividades relacionadas con el comando.

(2) Canal de EM.- Es el enlace entre los EEMM de coordinación de cuarteles generales diferentes. El EM usa este canal para controlar las actividades que se le relacionan y para coordinar y trasmitir información de planeamiento, instrucciones de control y otra información para apoyar el comando y control, tal como la red de operaciones e inteligencia o la red logística – administrativa.

(3) Canal técnico.- Es el enlace técnico entre dos comandos similares dentro de un comando más grande o entre EEMM especiales. Los canales técnicos son típicamente empleados para controlar actividades de apoyo de combate y apoyo administrativo que la organización más grande necesita; tales como en la red de dirección de tiro; comando, control, comunicaciones e inteligencia (C^3 I), etc.

15. TRANSFERENCIA DE LA INFORMACION

a. Las comunicaciones tácticas transfieren la información sobre todo el campo de batalla, por cualquiera de los canales de flujo de info, a través de cuatro categorías de información:

(1) Voz
(2) Mensajes
(3) Datos
(4) Imagen

b. Voz.- El tráfico de voz será proporcionado en tiempo real a través del flujo de información, de tres maneras:

(1) De usuario a usuario.- mediante el tráfico interactivo bidireccional.

(2) Por método conferencia.- cuando algunos grupos están conversando simultáneamente.

(3) Teledifusión.- cuando una vía o promotor se dirige a un gran número de receptores o destinatarios en un área amplia o considerable.

c. Mensajes.- Son informaciones en cualquier tipo de papel tales como documentos, cartas, mapas, calcos y fotografías. El tráfico de mensajes a su vez se clasifica en:

(1) Formal.- cuando es pasado a través del sistema de registro de correspondencia.
(2) Informal.- cuando es pasado directamente entre usuarios, por ejemplo empleando facsímil.

d. Datos.- Son informaciones digitales pasadas de máquina a máquina (computadoras). Cuando las computadoras están enlazadas entre ellas para pasarse info o compartir recursos, se constituyen en una red de computadoras. La trasmisión de datos incluye: tráfico de registros, facsímil, correo electrónico, transferencia de bases de datos, etc).

e. Imagen.- Son informaciones digitales transferidas por redes de comunicaciones transportando imágenes en tiempo real o en tiempo casi real sobre personas, lugares de campo de batalla o de otros objetos de interés. Puede ser de vídeo lento o "full motion".

16. FORMAS DE TRANSFERIR INFORMACION

El apoyo de Telemática para transferir la información a través de las tres categorías de la info, se realiza en una de las dos formas siguientes: usuario común o usuario exclusivo. La forma a emplear dependerá de las necesidades y escalón del usuario:

a. Usuario común.- Donde todos los usuarios de un sistema de comunicaciones tienen acceso a un gran grupo de suscriptores con mínimo recursos de comunicaciones.

b. Usuario exclusivo.- Donde se proporciona un enlace entre dos puntos, debido a la alta prioridad de la información a transferir o que el alto volumen del flujo de info impide compartir los enlaces de usuario común. Esta forma de transferencia ya no es practicable emplearla en los niveles tácticos, debido a que la tecnología de los equipos con que cuenta el ejército demandan compartir frecuencias y circuitos. Para niveles estratégicos y/o conjuntos, el empleo de enlaces satelitales, proveerán circuitos para usuarios exclusivos sobre estos sistemas.

17. CONCEPTUALIZACION Y DESCRIPCION GENERAL DE SISTEMAS DE COMUNICACIONES

a. Tradicionalmente ha sido conceptualizado a los sistemas de comunicaciones como al conjunto organizado de personal, medios de enlace, facilidades y técnicas, tácticas y procedimientos (TTP´s) de comunicaciones; para responder a los requerimientos de C^2 de una fuerza para el cumplimiento de la misión.

b. Hoy en día esta conceptualización no ha variado en esencia, pero el auge de la tecnología de la información, han agregado a los sistemas de comunicaciones los componentes de computación e información, para convertirse simplemente en sistemas de información (SINFOR).

c. El sistema de comunicaciones, para el combate, deberá poner énfasis en la dispersión, movilidad y flexibilidad que hoy en día deben poseer la fuerzas; para responder a las necesidades de enlace del comando con redes y sistemas confiables, seguras, flexibles, integrales y sincronizadas.

d. Organización de un sistema de comunicaciones

(1) La célula más pequeña de un sistema de comunicaciones es el medio y el hombre que la opera, pudiendo haber varios medios con un solo operador dependiendo de los tipos de medios y de la tecnología de los mismos.

(2) Al conjunto de células se le llama equipo, que pueden constituirse en órgano de comunicaciones en si mismo o ser parte de un órgano dependiendo del medio.
(3) Cuando los órganos de comunicaciones están dispuestos apropiadamente de acuerdo a la situación, misión, enemigo, terreno, tropas y tiempo (METT-T) se constituyen u organizan en un sistema de comunicaciones.
(4) Como la organización de un sistema de comunicaciones es dependiente de los factores METT-T; es decir, deben adaptarse a la maniobra, escalón de la fuerza que apoyan, área de cobertura, etc; entonces existirán diferentes sistemas útiles o explotables para cada situación.
(5) A pesar de lo expuesto, la organización de un sistema de comunicaciones deberá partir de una base general y común que puede adaptarse rápidamente a cualquier situación. Esta base general y común lo constituyen las normas generales de apoyo de Telemática ya tratados en el capítulo anterior y las necesidades básicas de enlace, entre otros aspectos por considerar (composición y tipo de órganos de comunicaciones, clasificación y características técnicas de los medios, etc).

e. Necesidades básicas de enlace
(1) Externas
(a) Con el escalón superior
(b) Con los elementos/unidades adyacentes
(c) Con los elementos de otros institutos/dependencias
(2) Internas
(a) Con las unidades subordinadas orgánicas, asignadas, agregadas y/o de refuerzo.
(b) Con los elementos de apoyo administrativo.

f. Composición y tipo de órganos de comunicaciones
(1) Un órgano de comunicaciones es el conjunto organizado de personal y medios de comunicaciones encargado de una función determinada de comunicación.
(2) El cmdo expone sus necesidades de enlace y el G-6/S-6 y/o el cmdte de la unidad de comunicaciones que lo apoya las satisfacen, suministrando los medios y el material constituido en equipos.
(3) La composición y tipo de los órganos de comunicaciones es variable dependiendo de tarea/misión y del medio a emplear. En el capítulo 3 se describen las organización de comunicaciones y forma de empleo de las mismas.

g. Medios de comunicaciones
(1) Ningún medio de comunicación será considerado como esencial, dependiendo el empleo de cada uno de ellos de los factores METT-T y de la disponibilidad del mismo. De acuerdo a ello se pueden clasificar en:
(a) Cable/alámbricos
(b) Radioelectricos/inhalambricos (mono y multicanal).
(c) Visuales/ópticos
(d) Sonoros/acústicos
(e) Mensajeros
(f) Animales amaestrados

(2) Todos estos medios deberán reunir ciertas condiciones básicas, que son:
  (a) Continuidad en su funcionamiento o confiabilidad
  (b) Secreto
  (c) Rapidez
  (d) Flexibilidad

(3) Por otro lado, todos los medios tienen sus características, posibilidades, ventajas, desventajas y limitaciones, que junto a la falta de disponibilidad de los mismos; posiblemente no satisfagan plenamente todas las necesidades de enlace de manera individual, sino que será necesario un empleo balanceado de todos ellos. A continuación se describirá brevemente cada una de las características, posibilidades, ventajas, desventajas y limitaciones:
  (a) Medios alámbricos/cable
    1. Características
      a. Puede ser interconectado para facilitar los enlaces locales
      b. Emplea el cable y alambre de campaña, teléfonos y centrales telefónicas, para facilitar el enlace
      c. Puede enlazarse con terminales de Teletipo
      d. Alarga las posibilidades de los abonados desde terminales Multicanales y ofrece rutas de trasmisión para enlaces Multicanales.
      e. Puede ser integrado a Sistemas de Radio (IRA)
    2. Posibilidades
      a. Más seguro que el radio
      b. Reduce las posibilidades de interceptación del enemigo
      c. Medio adecuado para solucionar enlaces, durante el cruce de ríos.
      d. Se puede explotar e integrar a los circuitos telefónicos comerciales.
      e. Medio más adecuado para ser empleado durante la defensa.
      f. Dobla a las comunicaciones radiales.
      g. Medio más adecuado para conducir ataques de sorpresa.
    3. Ventajas
      a. Las comunicaciones alámbricas proporcionan enlace directo entre persona y persona, tiene la facilidad de interrumpir el mensaje para aclararlo, no necesitando para ello esperar el término del mensaje.
      b. Es un medio relativamente seguro. Sin embargo no garantiza el Secreto del Mensaje.
      c. Su empleo es posible en todo terreno y estado atmosférico.
      d. Su operación es sencilla, no requiere especialistas y sus instalaciones relativamente rápidas y fáciles
      e. Racionalización que permite enviar varios mensajes por una sola línea utilizando el sistema multipar.
      f. Es el medio de comunicación más confiable.
    4. Desventajas
      a. Su instalación demanda tiempo y esfuerzo, sin embargo el tiempo y el esfuerzo pueden disminuirse con un apropiado plan de entrenamiento.

b. Son muy vulnerables y demandan gran cantidad de personal para su mantenimiento. De allí que debe tomarse todas la precauciones por nuestro personal, para no interrumpirlo, y el personal de construcción debe escoger rutas que hagan menos vulnerables, las instalaciones.
c. Difícil obtención.

5. Limitaciones
   a. Comparado con el radio, requiere para su empleo de mayor cantidad de tiempo, hombres así como más tiempo para su mantenimiento, instalación y operación del sistema.
   b. Hay pérdida de señal, cuando se establece enlaces a largas distancias.
   c. Sujeto a ser dañado por vehículos a ruedas u orugas
   d. Susceptible a ser interceptado, realizando apropiaciones y conexiones en los cables.
   e. Medio inadecuado para enlazar a Unidades altamente Móviles.

(b) Radio monocanal

1. Características
   a. Permite realizar comunicaciones inalambricas y que puede operar mientras se desplaza.
   b. De instalación rápida y puede tramitar un número apreciable de mensajes.
   c. Permite el enlace Tierra-Tierra, Aire-Aire y Tierra –Buque.
   d. Se emplea en Fonía, Radiotelegrafía, Radioteletipo y multicanal.
   e. Los tipos de modulación que emplea son: Amplitud Modulada (AM), Frecuencia Modulada (FM) Y Banda Lateral (BL).
   f. Las frecuencias primarias son: Alta frecuencia (HF), Muy Alta Frecuencia (VHF), Ultra Alta Frecuencia (UHF), Super Alta Frecuencia (SAF) Y Frecuencia Extra Alta (EHF).
   g. Las rutas de trasmisión incluyen: Onda Terrestre, Onda espacial, Línea de Vista y dispersión troposférica.
2. Posibilidades
   a. Puede alcanzar grandes distancias
   b. Puede operar a control remoto
   c. Puede emplearse como medio de retrasmisión para aumentar su alcance y/o vencer obstáculos.
   d. Requiere de poco esfuerzo operativo y ocupa poco espacio.
   e. Se puede integrar con el sistema telefónico.
3. Ventajas
   a. Rapidez de Instalación.- La principal ventaja de los medios Monocanales son su rapidez de instalación, radios portátiles y vehiculares pueden entrar en operación en cuestión de segundos.
   b. Flexibilidad.- Son medios flexibles, no requieren de circuitos fijos para instalarlos, operarlo y mantenerlos. Los puestos pueden agregarse o quitarse de una red de acuerdo a las necesidades.

c. Continuidad.- Las comunicaciones pueden mantenerse durante el desplazamiento de la Tropa.
d. Integración.- Pueden ingresarse con los medios Alámbricos y enlazarse de tierra a aire o de Aire a tierra (Integración Radio Alámbrica IRA).
e. Enlace en terreno difícil.- Proporciona comunicación en terreno que es imposible instalar medios alámbricos (selva, montaña, desierto, pantanos, etc).

4. Desventajas
a. El radio es el menos seguro de los medios, por la indiscreción a que está expuesto. Debe tenerse presente que la interceptación puede realizarse en cualquier momento, sea para captar sus mensajes o determinar la ubicación de estaciones de radio.
b. Es menos vulnerable al fuego con respecto al alámbrico, pero puede ser interferido por la estática, o por otros medios.
c. De difícil obtención y su operación requiere entrenamiento previo.
d. Estas desventajas pueden ser grandemente disminuidas mejorando la técnica del operador, en la explotación de procedimientos de radiotelefonía y seguridad de comunicaciones.

5. Limitaciones
a. Es influenciado por condiciones de propagación y el terreno.
b. Es el medio más vulnerable de comunicaciones, cuando no funciona en seguridad.
c. Puede ser interferido e interceptado.
d. Puede ser sometido a operaciones de engaño
e. Sujeto a interferencias atmosféricas, de tierra o de fuentes artificiales.
f. Su operación requiere de frecuencias comunes, equipos compatible y alcance óptimo.

(c) Radio multicanal

Los sistemas multicanales, son empleados para proporcionar enlace en la zona de operaciones, desde las GGUUCC hacia el EO, formando el sistema de área de usuario común. Los enlaces de radio multicanales, usan el sistema de trasmisión en multiplex que permite la tramitación de varios canales de comunicación en duplex y por consiguiente trasmisión de varios mensajes al mismo tiempo. Los pasos de comunicación (terminales) pueden ser interconectados a sistemas alámbricos y/o radiotelefónicos.

1. Características
a. Alta eficiencia y confiabilidad
b. Es adecuado cuando se requiere disponer de un mayor número de canales.
c. Simultaneidad de comunicaciones en fonía, grafía, telex, facsímil y preparado para teleproceso.
d. Reduce el costo de mantenimiento y cable.
e. Comunicación de línea de vista.
f. Realiza enlaces a grandes distancias
g. Rapidez de Instalación

2. Posibilidades
   a. Comunicación multicanal simultáneo de 12 a más canales
   b. Permite comunicación telefónica automática del PC de las GGUUCC con el CTO.
   c. Adecuado para solucionar enlaces a grandes distancias
   d. Puede ser incrementado mediante apropiación de circuitos a lo largo del sistema
   e. Su empleo se realiza en seguridad
   f. Permite comunicación en fonía, grafía, telefax y de datos.
3. Limitaciones
   a. La pérdida de la señal en el cable o radio, bajará el rendimiento de todos los circuitos.
   b. Es equipo pesado y que reduce su movilidad, por lo que debe estar montado sobre vehículos
   c. Requiere de mucha energía eléctrica para su funcionamiento.
   d. Requiere de personal entrenado.

(d) Audiovisuales

Las actividades audio visuales, tiene que ver con las comunicaciones que emplean dispositivos, ilustraciones gráficas, sonido, cine y televisión. El papel de los medios audio visuales comprende el registro, producción, almacenamiento y recuperación, distribución y presentación de imágenes visuales, sonido e intervención oral.

1. Características
   a. Proporcionar la información en apoyo de operaciones tácticas tales como: Reconocimiento aerofotográficos, informaciones que ayude a tomar decisiones al comandante y presentación de informaciones del G-2
   b. Es un medio importante para realizar el entrenamiento del EM y Jefes de Unidad
   c. Medio utilizado preferentemente para conducir operaciones sicológicas
   d. Medio utilizado en apoyo de actividades de información en el Ejército.
2. Posibilidades
   a. Permite registrar toda la información
   b. Uniforma el entrenamiento en las GGUU
   c. Proporciona películas de vídeo y/o fotografías
3. Ventajas
   a. Constituyen medios suplementarios de los otros
   b. Transmiten mensajes pre-establecidos
   c. Poco voluminoso y operados con facilidad
4. Desventajas
   a. Su empleo está subordinado al terreno y a la condición atmosférica
   b. Alcance corto y poco rendimiento
   c. Necesidad de códigos de mensajes pre-establecidos

5. Limitaciones
   a. Se requiere de mucho tiempo para prepararlos, de acuerdo a los requerimientos tácticos
   b. Es inadecuado para el apoyo en la condición de operaciones
   c. La limitación del procesamiento de películas en blanco y negro, que generalmente requieren de mucho tiempo.

El empleo de comunicaciones sonoras y visuales siguen siendo cada vez más importantes conforme aumenta las actividades de GE. En todas las armas colectivas, se da mayor énfasis al uso de medios visuales y sonoras durante el entrenamiento.

1. Características
   a. Puede ser utilizado en todo momento
   b. Dispone de numerosos recursos como son: Paineles, banderines, bocinas, campanas, silbatos, disparo de armas, sirena, etc.
2. Posibilidades
   a. Empleando para señalar ubicaciones
   b. Buen método para tramitar comunicación a grupos extensos o a unidades aisladas mediante códigos.
   c. Adecuados para coordinar los pasajes de línea.
   d. Utilizadas para conducir operaciones de enlace.
   e. No necesita energía eléctrica.
   f. No se emplean emisiones electromagnéticas.
3. Limitaciones
   a. Fácilmente puede ser mal interpretada.
   b. Puede ser interceptada por el enemigo.
   c. El enemigo puede usarlos para engañar
   d. Su uso es restringido cuando la viabilidad es reducida y cuando se conducen operaciones de combate.
   e. Las comunicaciones sonoras pueden ser confundidas con otros sonidos producidos durante el combate.

(e) Integración radio-alámbrica

Es el acoplamiento mediante una interfase que permite integrar las facilidades de los medios alambricos y las de radio, los que a su vez son interconectados a los tableros y/o centrales telefónicas y desde allí es utilizado por los abonados telefónicos.

1. Características
   a. Proporciona flexibilidad a las comunicaciones.
   b. Proporciona velocidad a los enlaces.
2. Posibilidades
   a. Medio para solucionar enlaces de emergencia
   b. Puede ser conectado y proporcionar enlace a grandes distancias.
   c. Empleado para dar continuidad a las comunicaciones móviles
   d. Efectivos durante la conducción de operaciones de cruce de ríos.
3. Limitaciones.- Las que corresponden a los medios alámbricos e inalámbricos.

(f) Mensajeros

Los mensajeros tienen la misión de llevar y traer documentos por medios físicos. Estos son empleados con mayor frecuencia cuando se tienen que llevar cartas, documentos, calcos, etc, que no se pueden trasmitir por otro medio o que podrían ser interceptados por el enemigo.

1. Características
   a. Se distinguen en todas las Unidades
   b. Es un medio confiable y flexible
   c. Es uno de los medios más seguros que se dispone en las unidades.
   d. Son de dos (2) tipos: mensajeros a horario y mensajeros especiales.
   e. Estos mensajeros pueden ser clasificados según el medio de locomoción que emplean: motorizado y aéreo.
2. Posibilidades.- Lleva y trae mensajes largos, cartas de gran tamaño y gran número de mensajes de rutina, o mensajes de emergencia y alto grado de seguridad.
3. Limitaciones
   a. Requiere de mayor tiempo para entregar y recibir mensajes
   b. Sujeto a la acción del enemigo (capturado)
   c. Sujeto a la disponibilidad del medio de transporte
   d. No hay conversación de persona a persona.

18. SISTEMAS DE COMUNICACIONES PARA LA RED DE INFORMACION DEL COMBATIENTE

a. La infraestructura de los sistemas de comunicaciones debería implementarse desde los niveles nacional y estratégico, para apoyar a los SINFOR de la red de info del combatiente (RIC) (Ver párrafo 12.c de este manual). Esta infraestructura, son una serie de redes de comunicaciones que constituyen la arquitectura de los sistemas de información cuando se integra con la disciplina de automatización.

b. Como se explica en el manual de operaciones de información (párrafos 56 y 57) y en el manual de empleo de comunicaciones satelitales en el ejército, la arquitectura de los SINFOR militares buscan integrar las comunicaciones con los sistemas automatizados del campo de batalla (SAC´s) para enlazar funcionalmente a los cuarteles generales estratégicos, operacionales y tácticos en una red integrada, interoperable y cohesiva. La estructura de esta red para el ejército se basa en las categorías de los SINFOR siguientes:

   (1) Sistema de C^2 global conjunto (SC^2 GC); o también denominado sistema global de C^2, que es el principal sistema de información de C^2 del combatiente de nivel nacional y/o conjunto, interfaceando con el sistema de comando de batalla del ejército (SCBE).

   (2) Sistema de comando de batalla del ejército (SCBE), que es el principal SINFOR de C^2 del combatiente del ejército, empleando una mixtura de redes móviles e instalaciones fijas o semifijas, dependiendo del subsistema. Comprende a tres sub-sistemas, según el escalón o nivel:

      (a) Sistema de C^2 global del ejército (SC^2 GE), que es un sistema de C^2 casi perfecto que opera en los altos escalones apoyando a los comandos de componentes terrestres, comando de teatro de

operaciones (si es del ejército) y de teatro de la guerra (si hubiera más de uno):

1. Este SC^2 GE debería ser interoperable con sistema de C^2 conjuntos y combinados a través de todo el rango de las operaciones militares y sistemas operacionales del campo de batalla (SOC´s).
2. Debería estar vertical y horizontalmente integrado en los niveles táctico y operacional, proporcionando conectividad para las bases de datos de información de combate y para los procesos de información pertenecientes a cada SOC´s.

(b) Sistema de C^2 táctica del ejército (SC^2TE), que es la integración de las disciplinas de comunicaciones y automatización, conocido en nuestro medio como telemática; para proporcionar apoyo a los SOC´s (maniobra, apoyo de fuegos, defensa aérea, comando de batalla, inteligencia, guerra electrónica, movilidad y supervivencia, y apoyo administrativo) que permita enlazarse directamente al SC^2GE y proveer un marco de conectividad casi perfecto desde niveles GU hasta DE y/o EO:

1. Estos SOC´s deberían ser apoyados por sistemas de información funcionales denominados sistemas automatizados del campo de batalla (SAC´s), que consisten de hardware y software de computadoras que organizan y manejan la info del campo de batalla que los cmdtes y sus EEMM necesitan (voz, mensajes, datos e imagen).
2. Los SAC´s son los medios de los sistemas de información automatizados (SIA) usados por los cmdtes y sus EEMM para recibir y distribuir info crítica entre fuerzas de diferentes escalones, institutos y hasta países. Sobre un campo de batalla moderno, las necesidades de transferencia de info crítica existirá en todos los escalones, donde el tráfico de voz y distribución de datos llegarán a ser los principales métodos para pasar esta info; sin embargo en algunas ocasiones los mensajes y la trasmisión de imágenes o vídeo también será necesaria.
3. El G-6 deberá prever y planear los medios que interconecten y comuniquen los SAC´s, de manera continua, segura y precisa; proporcionando info relevante e inteligencia sobre la conciencia situacional y cualquier otra info reunida, procesada y difundida, hacia y desde el cmdte, su EM y sus escalones superior y subordinados.
4. El primer reto será el desarrollo de capacidades de una internet táctica para establecer el uso y distribución de las nuevas posibilidades de las OI que hoy en día son posibles, debido a que el ejército ha iniciado la digitalización de todos sus sistemas de comunicaciones y muchas armas y servicios están introduciendo el empleo de sistemas digitales en sus unidades tácticas.
5. Esta internet táctica deberá contar con arquitecturas operacional y de SINFOR; la arquitectura operacional será necesaria para la conectividad de los elementos de la fuerza y por el tipo y volumen de info digital conformada por los

elementos dentro de la fuerza; y la arquitectura del SINFOR será para hardware y software específico que provea conectividad y difusión de info del cmdo de batalla. Las dos arquitecturas envolverán versiones para que usuarios predeterminados intercambien necesidades de info a través de la fuerza.

6. Cada nodo de la internet táctica deberá poder proporcionar servicios de información mientras se está en movimiento. La administración de la red deberá ser una característica importante de la internet táctica y será altamente crítica para el éxito de la entrega de info a través del campo de batalla, posibilitando al administrador de la info táctica monitorear y seguir a los usuarios tácticos sobre el campo de batalla. Cada nodo proveerá una herramienta para asesorar en la configuración dinámica que las redes de información del cmdo de batalla necesitan para conducir sus OI tácticas.

(c) Sistema de comando de combate de división y menores (SCCDM),

1. En términos cortos; el SCCDM empleará los sistemas de posicionamiento y navegación (GPS) y las comunicaciones sobre: sistemas de radio monocanal terrestres, tierra-aire-tierra, sistema de reporte de ubicación posición computado (EPLRS: enhanced position location reporting system), equipo terminal móvil de usuario (ETMU) y red de paquete táctico (MSE/TPN: mobile subscriber equipment/tactical pocket nerwork).
2. Estos sistemas formarán una red integrada que moverá la información (datos) entre los escalones superiores y subordinados (verticalmente) y entre organizaciones adyacentes o vecinas (horizontalmente), sin necesidad de tener que ser enrutadas a través del PC o cuartel general de la GU.
3. Los SCCDM deberán proporcionar conectividad digital desde el PC de la división hasta los sistemas de armas. La integración de los sistemas GPS, radios monocanal/EPLRS (o TACTER's) y MSE/TPN; para conformar una red homogénea y sistema de sistemas constará de:
   a. **Terminales tácticos (TACTER)**.- Una familia de computadoras de tamaño laptop conectada a equipos de navegación y radios, para proveer procesamiento y posibilidades de proyección o visualización a plataformas sin un procesador interno.
   b. **Internet táctica**.- Sistemas de comunicación de campo de batalla en red, empleando protocolos de internet comerciales.

c. Todos estos sistemas (expuestos en el subpárrafo "b") conjuntamente con los de otros institutos armados y redes/sistemas del estado, deberían constituirse en la " Red de Sistema de Información de Defensa (RSID)"; con capacidad de proporcionar conectividad de larga distancia, conmutación y servicios de telecomunicaciones para transferencia de info entre todos los puestos de comando, áreas de servicios, zonas del interior y de combate; sea que los elementos por apoyar estén en lugares fijos, desplegados o desplazándose. Esta red deberá apoyar cualquier tipo de operación militar, incluyendo el apoyo a defensa civil en desastres naturales, asistencia de

acción cívica en zonas aisladas del territorio nacional, operaciones contra el tráfico ilícito de drogas en regiones selváticas y/o montañosas, y en lugares fuera de nuestro territorio cuando nuestras fuerzas actúen como parte de operaciones de paz.

d. La RSID incluirá la infraestructura (de trasmisión y conmutación) necesaria para proporcionar apoyo de Telemática de conmutación segura y no-segura, tráfico de voz punto a punto y punto a multipunto, distribución de datos y servicios de mensajes imagen/vídeo; empleando una combinación de redes militares y no-militares (comerciales):
   (1) Voz.- Los servicios de conmutación de voz (segura y/o no segura) permitirán conexiones entre ubicaciones de la RSID, incluyendo conmutación de voz de larga distancia, Telefacsímil y llamadas de conferencia. La idea es integrar todos los centros o centrales de conmutación fija de todas las fuerzas armadas, policiales y otras dependencias de defensa en una sola, empleando soportes de trasmisión fijos o radiales, seguros y no- seguros, inclusive para aquellas fuerzas que se desplieguen a zonas de operaciones. En este último caso necesariamente deberá ser segura, con redes de conmutación digital inhalambricas con criptografiado de voz interno y externo, que provea servicios de voz segura de alta calidad, datos y comunicaciones en conferencia para los cmdtes de escalones superiores que deban tomar decisiones. La red para el tráfico de voz deberá ser capaz de soportar llamadas de señalización especial desde 2.86 Khz, 56 Kbps y 64 Kbps de voz, dato y vídeo digital sobre T1 o E1(dependerá de tecnología que se adquiera), visando alcanzar o lograr las interfaces de protocolo PRI (primary rate interface) de una red digital de servicios integrados (RDSI).
   (2) Conmutación de datos.- Los circuitos para servicios de conmutación de datos originan y terminan conexiones de datos entre servicios conmutados y acceso a puntos de entrega de servicios.
   (3) Datos empaquetados punto a punto.- Los servicios de datos empaquetados (roulers de red de protocolo internet) emplearan la RSID para una trasmisión continua de estos paquetes. Lo ideal sería contar con redes físicas de conmutación ATM (Asynchronous Transfer Mode), que ya existe en el país, particularmente para soportar las redes WAN´s e interconectar puntos de entrega de servicios de redes LAN.
   (4) Servicios de mensajería.- A través de la red de correo electrónico del ejército y de ser posible con algún otro "servicio de valor agregado", a través de la red conmutada del ejército y/o de defensa (cuando se logre la integración total como RSID.
   (5) Servicios de vídeo.- La vídeo-teleconferencia permitirá que dos o más ubicaciones se comuniquen en tiempo real empleando información de audio y vídeo. Estos servicios pueden ser punto a punto o punto multipunto, con conectividad dedicada o discado; y con facilidades adicionales como un centro de reservación y conexiones a otras redes:
      (a) Estos servicios normalmente serán proporcionados en guarnición, dentro del territorio nacional, empleando una combinación de red comercial y red militar (donde existan backbone de fibra óptica o redes radiales digitales de alta capacidad o ancho de banda).
      (b) Deberá preverse por lo menos una "hub" de vídeo en cada región militar, las que contarán con todos los "puentes" necesarios de

hardware y software para proporcionar la conectividad requerida. Todas las trasmisiones de vídeo (con excepción de las de punto a punto y discado) deberán pasar a través de estas “hubs”.

(c) Las centrales de conmutación telefónica de AT&T con que cuenta actualmente el ejército tienen la posibilidad de proporcionar servicios de vídeo teleconferencia, con lo cual se podría obviar algunas “hubs”, dependiendo de la tecnología empleada.

(d) Mayor información y detalles sobre estos servicios se podrán encontrar en manuales que se están preparando en la Escuela de Comunicaciones.

e. De todos los sistemas expuestos en este párrafo este manual tratará con detalle el SC^2TE, en el párrafo siguiente.

19. SISTEMA DE COMANDO Y CONTROL TACTICO DEL EJERCITO (SC^2 TE)

a. La arquitectura del SC^2 TE deberá visualizar, desarrollar y establecer un conjunto de redes y sistemas de comunicaciones tácticas que se dividan en las redes WAN´s siguientes:
   (1) Sistema de comunicaciones de área de usuario común (SCAUC)
   (2) Sistema de redes de radio monocanal de combate (SRMC)
   (3) Sistema de distribución de datos del ejército (SDDE)
   (4) Sistema de comunicaciones de teledifusión del ejército (SCTE)

b. Sistema de comunicaciones de área de usuario común (SCAUC)
   (1) El SCAUC es un sistema de comunicaciones que deberá ser diseñado a base de una serie de centros de conmutación digital nodal de red, conectados entre sí principalmente con radios multicanales digitales de línea vista y terminales satelitales tácticos; fundamentalmente para apoyar a escalones División de Ejército y Ejército de operaciones.
   (2) Para escalones de gran unidad de combate (GUC) y menores se deberán emplear equipos terminales móviles de usuarios (ETMU), que en red también constituyen un sistema nodal de conmutación de voz y comunicación de datos, de usuario común que se extiende mediante componentes de receptores/trasmisores para proporcionar cobertura de área, pero de menor capacidad que los sistemas que apoyan al EO/DE.
   (3) El SCAUC, deberá contar con sistemas de conmutación electrónica, móviles, automáticos y modulares; totalmente digitales, seguros y altamente flexibles; que proporcionen un sistema multiusuario y de área de uso común para comunicaciones de voz y de datos para fuerzas desde el nivel EO hasta batallones inclusive. Los usuarios que estuvieran en el área de extensión de los nodos o cerca de ella, se enlazarán a los subsistemas, para accesar a otros usuarios de la misma área o de otras áreas:
      (a) El corazón del subsistema de comunicaciones que apoya al EO/DE serán conmutadores de circuitos digitales apoyados por soportes de trasmisión (radio multicanal y/o sistemas satelitales) que tipicamente tengan capacidad para trasmitir y conmutar desde 4 hasta 144 canales full-duplex, proporcionando a los suscriptores (usuarios) con conectividad a sistemas estratégicos (SC^2GE y/o SC^2GC) redes de ETMU y redes comerciales, debiendo ser interoperable con las redes de otros institutos.

(b) Las redes de ETMU deberán contar con facilidades que permitan la movilidad del combatiente al mismo tiempo que minimiza el impacto de sobrecarga de tráfico y enlaces o perdidas de servicio de elementos funcionales, empleando direcciones y suscriptores discretos como un medio para intercambiar info de C^3I en un ambiente táctico dinámico.

(4) Las características técnicas, posibilidades, limitaciones y formas de empleo de los equipos de radio multicanal y terminales de satélites tácticos, están desarrollados en manuales técnicos específicos. De igual forma los conmutadores digitales de gran capacidad para empleo en escalones de DE/EO y de las ETMU también serán desarrollados ampliamente en manuales técnicos específicos, sin embargo en este manual en una sección especial se hará un resumen comprensible de los ETMU, y de los equipos de radio multicanal digitales.

c. Sistema de redes de radio monocanal de combate (SRMC)

(1) Cada red de radio monocanal de combate, se constituirá en la principal estructura de red de comunicaciones dentro del concepto de internet táctica (IT). La internet táctica es una red consistente de radios tácticos y hardware/software del computador que provee la principal arquitectura de comunicaciones para apoyo de Telemática al combatiente en los escalones GUC y menores.

(2) Esta red de IT deberá permitir compartir datos de C^2 por los cmdtes, sus EEMM, las unidades como tales, los soldados individualmente y las plataformas de los sistemas de armas; dando como resultado una conciencia situacional en tiempo casi real; y, mejorando el C^2 de la fuerza mediante el incremento de la letalidad, el ritmo de las operaciones y la supervivencia.

(3) La IT es básicamente los computadores de los sistemas de comando de combate de división y menores (SCCDM), los sistemas de reporte de ubicación/posición computarizada (EPLRS: Enhanced Position Location Reportingg System) o terminales tácticos (TACTER), los equipos de radio de última generación (HF-2000, CRN 900 y satelitales tácticos portátiles), los nodos de pequeña extensión de los ETMU (NPE/ETMU) y todo el equipamiento de comunicaciones adicional que se requiera.

(4) La IT deberá convertirse en una herramienta muy importante para el cmdte de maniobra, proporcionando redes y sistemas de trasmisión que transporten la info que necesita para operar dentro del ciclo de planeamiento del oponente en un campo de batalla. Las herramientas de administración de red automática en los escalones batallón y GU de maniobra proverán posibilidades de planeamiento, monitoreo y reconfiguración de internet táctica.

(5) El elemento de control de sistemas de la GU usará la herramienta de administración de red y programas de administración comerciales “hechos” para administrar a la internet táctica, planeando e inicializando el “back bone” de los TACTER en conjunción con la estación de control de red y el NPE/ETMU. Este elemento proveerá info de red a las radios monocanal de combate para se revisen las instrucciones operativas de comunicaciones-electrónicas (IOCE) y la administración de frecuencias para las radios.

(6) Las redes de radio monocanal de combate como estructura soporte de la IT proverán conectividad casi perfecta entre radios de última generación para el tráfico de datos, acceso a las comunicaciones y para el backbone de los TACTER (EPLRS) vía un controlador de internet. Estas redes de radio deberán contar con subsistemas de seguridad de voz y salto de frecuencia compatible con el controlador de internet, de tal manera que permita conectar y pasar tráfico de datos entre dos redes de radio distintas. Para redes más grandes (tales como las de NPE/ETMU) se deberán emplear interfaces de usuario de multipuertos tácticos para proporcionar plataformas (backbone) de enrutamiento entre batallones y GGUU en una misma área.

(7) Mayor información sobre la internet táctica, las redes de radio monocanal de combate, los TACTER y los NPE/ETMU, se encontrarán en manuales técnicos específicos; sin embargo en secciones aparte se describirán sucintamente algunas de ellas.

d. Sistema de distribución de datos del ejército (SDDE)

(1) El SDDE es un sistema de comunicaciones de C^2 integrado que proporciona enlaces de datos en tiempo real o tiempo casi real, para redes de datos de baja y mediana capacidad (volumen de datos/velocidad de trasmisión), como parte de un sistema de distribución de datos (SDD) mayor.

(2) Este sistema retrasmite la información automáticamente desde el origen o remitente hasta el destino o destinatario, de manera transparente al usuario; proporcionando información sobre posición precisa, ubicación, navegación, identificación e informes de unidades sobre el campo de batalla.

(3) Los puestos terminales del SDDE deberán ser radio orgánicos y operados por los usuarios que son parte integral de sus sistemas de C^2. Estas radios deberán funcionar automáticamente para recibir o retrasmitir datos. La unidad de comunicaciones que apoye será la responsable por la administración y control de red, proporcionando equipamiento dedicado de retrasmisión para completar la conectividad de red.

(4) El SDD deberá consistir de dos subsistemas:

(a) Sistema de reporte de ubicación/posición computarizada (EPLRS)

1. Es un sistema de comunicaciones basado en computador (terminales tácticos: TACTER) con capacidad para proveer a los usuarios o suscriptores con trasmisión y distribución de datos seguro, resistente a la perturbación, libre posibilidad y en tiempo casi real. Proporciona también identificación de la unidad, ayudas de navegación e informe de ubicación automática de las fuerzas de combate táctico y de apoyo de combate. Nuestro ejército cuenta con parte de este sistema (el TACTER) , sin embargo el EPLRS completo emplea un equipo de radio con:
   a. Seguridad criptográfica con reenclavado en operación de nivel dual integral (CONFIDENCIAL/SECRETO)
   b. Salto de frecuencia
   c. Código de protección de error como protección electrónica.
2. Una red de EPLRS típica podría consistir de una estación de control de red y una cantidad variable de unidades usuarias

operando sobre ocho (8) frecuencias de UHF de (420 a 450 Mhz). Deberá contarse además con interfaces de computador "host" para conectar artificios de transferencia de datos hacia un ELRS de unidad usuaria; permitiendo dirigir la transferencia de info desde el computador trasmisor hacia el computador receptor a velocidades de 1.2 Kb/s; normalmente estos interfaces son el estándar X25.

3. Mayor información sobre las redes EPLRS se encontrará en los manuales técnicos y de empleo de dichos equipos.

(b) Sistema de distribución de información táctica conjunta (JTIDS: Joint Tactical Information Distribution System)

1. Son sistemas de radio avanzados que proveen comunicaciones para distribuir info y posibilidades de posición, localización e identificación principalmente para elementos defensa aérea; en una forma integrada aplicable a operaciones militares tácticas conjuntas.
2. El sistema distribuye info encriptada a altas velocidades y debe ser resistente a la perturbación en un ambiente electromagnético hostil. El JTIDS también proporcionará a los elementos de superficie y aerotransportados con posibilidades de posición/localización y una identificación básica a través de la distribución de posición segura e info de identificación.

e. Sistema de comunicaciones de teledifusión del ejército (SCTE).

(1) Son una serie de subsistemas de comunicaciones que emplean la tecnología similar a las estaciones de radio y televisivas comerciales. Sólo trasmiten las estaciones que envían información a través de sistemas radiales de HF, VHF o UHF, sistemas satelitales, vehículos aéreos no tripulados u otros medios de radiodifusión. Ejemplos de estos sistemas son los GPS's para navegación / ubicación de posición, pronósticos de clima e información o inteligencia sobre el terreno (sistemas geomáticos).

(2) Este sistema vendría a ser parte del servicio de difusión global (SDG) que está ampliamente expuesto en el ME11-70 (Empleo de las Comunicaciones Satelitales en el ejército) en sus párrafos 93 al 95.

SECCION II. SCAUC: EQUIPOS TERMINALES MOVILES DE USUARIO (ETMU)

20. INTRODUCCION A LOS ETMU

a. Los ETMU son parte del sistema de comunicaciones de área de usuario común (SCAUC) que apoya a escalones EO y menores, proporcionando un sistema de comunicaciones conmutado de usuario común que enlaza nodos de conmutación. Este sistema es digital, seguro y flexible que contiene características que compensan las necesidades de mayor número de enlaces, las pérdidas de enlaces, la sobrecarga en el tráfico y el rápido movimiento de los usuarios.

b. El ETMU provee comunicaciones de voz y datos sobre una base automática, direccionamiento discreto y directorio fijo, usando la técnica de búsqueda de ruta total; para apoyar o suscriptores móviles (radiales) o conectados por medios físicos (cable, alambre) con equipos para

intercambiar información de C^4 I. Adicionalmente cuenta con un paquete de conmutación de red, denominado Paquete de Red Táctico (PRT) que está insertado sobre la red de conmutación de circuito del equipo terminal móvil de usuario. Cuando los ETMU conforman una red, el PRT se convierte en el Paquete de Red de ETMU (PRE).

c. Cada ETMU viene montado sobre cabinas de vehículos multipropósito de alta movilidad, con capacidad de interconectarse a equipos de radio multicanal digital, terminales satelitales tácticos, cable y/o fibra óptica; tanto de redes militares como comerciales. Esta interconexión tiene por objeto proveer posibilidades de mayor alcance de los ETMU.

d. Cuenta también con un sistema de control integrado (SISCONI) que proporciona a los Cmdtes de Unidades de Comunicaciones y a sus EEMM con una capacidad automática para planear, hacer la ingeniería y operar todas las redes y sistemas de comunicaciones disponibles a la Unidad de Comunicaciones. Este SISCONI también integra a la estructura de la unidad de comunicaciones en el sistema de comando de batalla del ejército (SCBE) para el apoyo de Telemática al C^2.

21. EMPLEO DE LOS ETMU

a. Los ETMU cuando están adecuadamente arreglados en red, pueden apoyar a un Ejército de operaciones (EO) de cinco (05) grandes unidades en una zona de operaciones (Z/O) de hasta 5,000 Km^2 formando una grilla o enmallado de redes que cubren esa zona.

b. Para una GU, la grilla o malla de ETMU consiste de tres a cinco centros nodales (CN´s) que constituyen el soporte o back bone de la red. Para un EO, existirán 16 CN´s que hacen su red.

c. Sobre toda el área de maniobra, los usuarios o suscriptores se conectan a extensiones de nodos pequeños (ENP) o extensiones de nodos grandes (ENG) por medios radioelectricos o cable/alambre. Estas extensiones sirven como centros de conmutación de llamada local y proveen acceso a la red mediante la conexión a un conmutador de centro nodal (CCN) en el CN.

d. El paquete de red de ETMU (PRE) apoya a las comunicaciones de datos dentro de un EO a los recursos de fuerzas de tarea conjunta, fuerzas adyacentes y grandes unidades, incluyendo su integración a redes comerciales existentes en la Z/O.

22. DESCRIPCION FUNCIONAL DE LOS PRINCIPALES COMPONENTES DE LA RED DE ETMU

a. Los ETMU tienen varios componentes integrados para asegurar a los suscriptores/usuarios móviles o estáticos que cuenten con capacidades de voz, datos, facsímil y algo de imagen. Estas capacidades apoyan a sus comunicaciones no importando donde ellas se encuentren en la red malla de ETMU de la Z/O. Los componentes principales de la red de ETMU incluyen:

(1) Centro nodal (CN)
(2) Conmutador de centro nodal (CCN)
(3) Extensión de nodo grande (ENG)
(4) Conmutador de extensión de nodo grande (CENG)
(5) Extensión de nodo pequeño (ENP)
(6) Conmutador de extensión de nodo pequeño (CENP)

(7) Unidad de acceso radial (UAR)
(8) Sistema de control integrado (SISCONI)
(9) Herramientas de administración de red (HAR)
(10) Sistema de radio multicanal de línea de vista
(11) Terminales de suscriptores/usuarios
(12) Conmutadores de entrada de la fuerza (CEF)

b. Centro nodal con conmutador de centro nodal

(1) Los CN´s proveen conmutación clave, control de tráfico y puntos de acceso para el ETMU. Después que se ha determinado el área de cobertura, los CN´s son asignados o distribuidos para establecer una red malla de ETMU del EO. Enlazados por radios multicanales de línea de vista, los CN´s proporcionan comunicaciones sobre todo el sistema vía los conmutadores de centros nodales (CCN´s) que se encargan de la conmutación y de los servicios de enrutamiento de desborde. Si un CN quedará inoperativo por cualquier causa, el sistema automáticamente enruta las comunicaciones a través de otro CN.

(2) Los CN´s sirven como un punto de acceso para los CENG´s, CENP´s, UAR´s y PRE´s: El CCN es el hub de un nodo de ETMU y provee interface de red para elementos de acceso de suscriptor/usuario, proporcionando la característica de ubicación automática del usuario que permite la asignación de dirección permanente y obvia la necesidad de conocer donde está físicamente localizado el suscriptor/usuario. Algunas características del CCN son:

(a) Está contenida en dos cabinas S-250, una para el grupo de conmutación y otra para el grupo de operaciones. Dichas cabinas van montadas sobre vehículos todo terreno y altamente móviles.

(b) El grupo de conmutación provee interface externa, conmutación de circuitos y funciones asociadas. El grupo operaciones provee el procesamiento central y funciones de interface del operador.

(c) El paquete de red de ETMU (PRE) provee:

1. Un puerto (gateway) de paquete de conmutación por CCN
2. Dos puertos para LAN (ambos de 802.3 y X25)
3. Hasta 64 troncales de 16Kbps cada una (sobre grupo troncal de 1024 Kbps entre una y otro CCN.

(d) Como terminaciones de líneas externas se tiene:

1. Digital: troncales y “loops” locales
2. Analógico: según se requiera
3. 16 grupos de trasmisión digital, 15 de las cuales pueden estar con artificios de encriptado de troncal

(e) Clusters de grupo troncal (CGT)

1. Cinco internodales
2. Seis de extensión de nodo pequeño (ENP)

(f) Dos unidades de acceso radial (UAR´s) por CGT

(g) Cuatro CGT asignables para cualquier combinación internodal, ENG, ENP, PRE o UAR/CGT´s.

(h) 24 “loops” locales para teléfonos digitales

(i) Un grupo electrógeno de 10KW

c. Extensión de nodo grande con conmutador de extensión de nodo grande

(1) La ENG proporciona comunicaciones de cable/alambre para el personal de un Puesto de Comando (PC) de nivel DE/EO. Una ENG permite conectar libremente hasta 164 suscriptores/usuarios vía

cable/alambre a través del conmutador de ENG (CENG) usando la técnica de búsqueda automática de enrutamiento por desborde. Los usuarios tienen acceso a los CN´s y al resto del ETMU vía los radio multicanal de LDV (Línea de vista) que conectan a los CENG´s mediante cable o radio SHF.

(2) Los CENG´s también proveen la característica de ubicación automática del usuario . Los CENG´s básicamente están configurados de la misma forma que los CCN´s, diferenciándose en la configuración de sus troncales y terminales, siendo sus principales características las sgtes:

(a) Está contenida en dos cabinas S-250, una para el grupo de conmutación y otra para el grupo de opns; cada una montada sobre vehículos todo terreno altamente móviles.

(b) Un CENG no es un conmutador "tandem" debido a que su uso principal no es ser un punto de conmutación intermedio entre otros centros de conmutación, pero si apoya a la búsqueda de enrutamiento por desborde y el gpo de conmutación también provee interface externa, conmutación de circuitos y funciones asociadas. El gpo opns también provee procesamiento central y funciones de interface del operador.

(c) Algunos CENG´s tienen la posibilidad que los usuarios de equipos de radio CNR 900 puedan entrar a la red de ETMU y proporcionarles acceso a la red comercial (concepto de integración radio-alámbrica)

(d) El PRE provee:

1. Dos puestos de paquetes de conmutación por CENG
2. Cuatro puestos para LAN (802.3 y X25)
3. Siete puertos X25 acondicionados para difase
4. Hasta 34 troncales de 16 Kbps cada uno o dos grupos troncales de 512 Kbps entre el CENG y dos CCN´s.

(e) Terminaciones externas:

1. Digital: Troncales y locales
2. Analógico: teléfonos comerciales

(f) Tres CGT encriptados:

1. Dos para diferentes CN´s
2. Uno asignable a una ENP.

(g) Capacidad de interfacear equipos de VHF de última generación

(h) Un grupo electrógeno de 10 KW

d. Extensión de nodo pequeño con conmutador de extensión de nodo pequeño

(1) El ENP proporciona comunicaciones de cable/alambre para el personal de un PC de nivel GUC, Agrupamiento, Destacamento, organización de tarea y hasta batallón. Una ENP permite conectar hasta 26 suscriptores/usuarios a través del conmutador de ENP (CENP) para proveerles enrutamiento y conmutación local. Los usuarios pueden tener acceso a los CN´s y al resto de la red de ETMU vía las radios multicanal de LDV que conectan a los CENP´s mediante cable o radio de bajada de altura (cerro, colina, edificio,etc).

(2) El ENP también provee funciones similares a un ENG cuando se conecta a un CCN/ENG, siendo sus principales características las sgtes:

(a) Está contenido en una cabina S-250 Especial, que está montada un vehículo todo terreno.
(b) El CENP consiste de equipamiento de conmutación, multiplexación y de seguridad de comunicaciones, pudiendo proveer una interface de red de radio digital segura.
(c) El CENP interfacea directamente con el CCN y CENG vía cable coaxial, radio multicanal de LDV o satélites tácticos multicanal.
(d) El PRE provee:
1. Un puerto de paquete de conmutación por CENP.
2. Dos puertos para LAN (802.3 y X25).
3. Cinco puertos X25 acondicionados para difase
4. Hasta 16 troncales de 16 Kbps cada uno sobre un grupo troncal de 256 Kbps entre el CCN´s o ENP.
(e) Terminaciones externas
1. Digital: Troncales y locales
2. Analógica: Teléfonos comerciales
(f) Conmutador digital de 26 terminaciones como mínimo
(g) Dos tableros de conmutación digitales pequeños (12 abonados como mínimo)
(h) Un CGT de 12 canales para un CN o ENG
(i) Capacidad para interfacear como radio monocanal VHF/HF
(j) Un grupo electrógeno de 10 KW

e. Unidad de acceso radial (UAR)
(1) Las UAR´s pueden seleccionar las Telemática de un terminal radiotelefónico de usuario móvil (TRUM) y enviarlas a los CN´s. Cuando un usuario se desplaza fuera del alcance de una UAR hacia otra, el servicio telefónico se transfiere automáticamente a la siguiente (nueva) UAR proporcionando así reafiliación automática. Cualquier llamada subsiguiente será colocada sobre el sistema vía la nueva UAR asegurando una total y continua afiliación funcional sobre toda la Z/O.
(2) La UAR se conecta directamente a un CN por cable o remotamente por radios de LDV. LA UAR local provee cobertura radial dentro del área general del CCN al que está conectado, mediante el establecimiento automático de comunicaciones seguras y full-duplex entre el TRUM y la red de ETMU. El alcance de planeamiento entre un TRUM y la UAR es de aproximadamente 12 Kilómetros dependiendo del tipo de terreno y potencia empleada.
(3) Algunas características generales de la UAR son:
(a) Ocho radios digitales.
(b) Capacidad de hasta 8 llamadas simultáneas de TRUM
(c) Un CGT de 256 Kbps usando 10 canales para CN.
(d) Rango de frecuencia de 30-88 Mhz.
(e) Full dúplex.
(f) Grupo electrógeno de 5 Kw

f. Sistema de control integrado (SISCONI)
(1) El SISCONI es un arreglo de hardware y software ensamblando en una cabina S-250 que esté montada sobre vehículo todo terreno, que da al Cmdte de la unidad de comunicaciones y a su EM la capacidad de automatización para realizar la ingeniería, planear y operar todos los sistemas de comunicaciones incluyendo a los ETMU.

(2) Esta capacidad permite al Cmdte interactuar con el sistema de comando de batalla del ejército (SCBE) mediante el intercambio de información de comando de batalla común con el cmdte de la fuerza y su EM; y, mediante el intercambio de información de comunicaciones con los G-6s/S-6's u oficiales de Telemática de la fuerzas de maniobra, apoyo de combate y/o apoyo administrativo.

(3) El SISCONI usa hardware y software común para sus estaciones de trabajo (Workstations). El software debería ser común para toda la infraestructura información del ejército (IIE).

(4) El SISCONI se extiende desde el NC hasta el SISCON del EO y Cuarteles Generales de menor escalón, proporcionando las herramientas necesarias para realizar el proceso de administración de la información de manera automática mediante las funciones siguientes:

(a) Planeamiento e ingeniería de red (PIR)
(b) Administración de las WAN's
(c) C^2 de Telemática
(d) Administración del espectro electromagnético de combate (AEC)
(e) Administración de la seguridad de comunicaciones.
(f) Administración del sistema.

g. Herramientas de administración de red (HAR)

(1) Las HAR proveen capacidad de SISCON del ETMU, monitoreando, manejando y configurando la red de ETMU (voz y datos) para unas comunicaciones óptimas. Estás HAR es un SISCON de comunicaciones integrado y computarizado que provee control de sistema automático y en tiempo casi real para apoyar al planeamiento, configuración, reconfiguración y monitoreo de la operación y movimiento de los recursos de ETMU.

(2) Los HAR se conectan normalmente a un CCN o CENG empleando cable PCM (pulse Code Mudulation). Las HAR consisten de una cabina técnica y otra para administración/planeamiento:

(a) La cabina técnica alberga una workstation para el centro de administración de red y otra workstation que provee proyección gráfica en tiempo casi real de la red de ETMU. El centro de administración de red monitorea y controla a las HAR. LA función principal de la workstation técnica es monitorear y asignar funciones de administración.

(b) La Cabina de administración/planeamiento alberga a los planificadores de red que completan las funciones de la cabina técnica, mediante dos workstations de administración del sistema que proveen proyección gráfica en tiempo casi real de la red de ETMU y las herramientas automáticas para crear y cambiar las bases de datos que se requieren para las operaciones de los ETMU.

(c) Las funciones de ambas cabinas trabajando complementariamente incluyen:

1. Administración del despliegue de equipos
2. Supervisión y administración de las HAR.
3. Administración de los límites.
4. Administración de material/equipo clave de SEGUCOM
5. Administración de equipos de VHF/UHF/SHF

6. Administración de base de datos de usuarios/suscriptores.
7. Administración de mensajes.

(3) Las HAR a nivel DE/EO pueden contar con una cabina adicional de administración/planeamiento. Adicionalmente pueden tener otra cabina de administración/planeamiento para soportar el incremento de la carga de trabajo en el planeamiento de red dentro de la Z/O de un EO.

(4) Algunas de las capacidades y/o características con que debieran contar las HAR son:
(a) Monitor de proyección de pantalla grande (52 pulgadas sería ideal)
(b) Mapas topográficas digitalizados.
(c) Administración/planeamiento de paquete de red de ETMU (PRE).
(d) Administración/planeamiento/distribución de frecuencias.
(e) Actualización automática de las HAR que están en espera (standby).

(5) Adicionalmente, las HAR en sus funciones de apoyo de administración/planeamiento, cuentan con una o dos herramientas de planeamiento de red (HPR); que proveen un mejoramiento al planeamiento e ingeniería de red (PIR) así como capacidades de administración de información operacional automatizada que incluyen:
(a) Parámetros ambientales.
(b) Digitalización de mapas.
(c) Ingeniería de sistemas radiales y de antenas.
(d) Análisis de perfiles del terreno.
(e) Emplazamiento de los recursos del sistema.
(f) Administración/asignación de frecuencias (VHF, UHF, SHF)
(g) Análisis de interferencia uno a uno.
(h) Análisis de amenaza de guerra electrónica.
(i) Administración de listas de usuarios/suscriptores.
(j) Programa de procesamiento de palabras.
(k) Programa de correo electrónico.
(l) Monitoreo de paquete de red

(6) Las HAR incluyen a las herramientas de software funcional siguientes:
(a) HPR para recursos de ETMU.
(b) Administración del espectro electromagnético de combate.
(c) Administración de la WAN de ETMU.
(d) Administración del sistema.
(e) Administración de correo electrónico (E-Mail)

(8) Las HAR pueden tener dos configuraciones dependiendo del área por cubrir, cantidad de usuarios/suscriptores y cargas de trabajo: una versión cuenta con un servidor u dos estaciones de trabajo/workstation (nivel EO) o una workstation (GU); la otra versión cuenta una sola workstation para unidad de comunicaciones y zona del EO/GU. Una versión mejorada de las HAR considera un SISCONI con dos servidores, cuatro workstation y hasta diez terminales remotos para apoyar a un EO.

h. Sistema de radio multicanal de línea de vista (SRMA/LDV)

(1) El SRMA consiste de enlaces versátiles que conectan todos los centros modales (CN's) en una red malla y provee servicios de conmutación automática para usuarios/suscriptores móviles o conectados físicamente.

(2) Esta red de malla radial entrega comunicaciones inhalambricas para cubrir áreas de grandes extensiones de kilometros cuadrados. Cada enlace radial cuenta con un alcance efectivo entre 25 a 40 Km, trabajando en bandas de frecuencias de 225-400 Mhz (banda 1/UHF y de 1350-1850 Mhz banda 3/SHF), sin embargo las frecuencias deberán ajustarse al plan de canalización y frecuencias asignadas por el Ministerio de Transportes y Comunicaciones al CCFA (ejército). Todos los equipos multicanales modernos vienen equipados con multiplexores de grupo digitales.

(3) El SRMA proporciona enlaces de radio punto a punto entre varios nodos de una red de ETMU. Las dos bandas le permiten establecer enlaces para alcances de hasta 40 Kms en la banda 1 (UHF) y enlaces cortos con Telemática de baja potencia en la banda 3 (SHF) para proporcionar conexión de bajada de altura hacia el sitio donde se ubica el PC o COT reduciendo el riesgo que significan los sitios donde se ubicarían los terminales de radio multicanal que trabajan en la banda UHF y que normalmente se ubicarán en lugares elevados para lograr la línea de vista. Cada enlace de radio provee una conexión única, full-dúplex y nivel-grupo; y, un canal digital de voz orderwire.

(4) Una versión de terminal de radio multicanal (TRM) se despliega típicamente con un conmutador de extensión de nodo pequeño (CENP) o una unidad de acceso radial (UAR) remota comportándose como terminal propiamente dicho; y, dicho TRM está equipado con dos radios (uno en banda 1 y otro en banda 3) y una antena mástil. El equipo de radio en la banda SHF opera en tandem con el radio enlace de UHF.

(5) Otra versión de TRM se despliega típicamente con un conmutador de centro nodal (CCN) y se comporta como radio relevador (dos funcionarían y uno de redundancia) y tres antenas mástiles. Cuenta también con la banda de SHF para conectarse a un PC que estuviera en la vecindad.

(6) Finalmente existe una tercera versión de TRM que típicamente se despliega con un conmutador de extensión de nodo grande (CENG) y está equipado con dos radios y dos antenas mástiles.

(7) Todas estas versiones y/o configuraciones de los sistemas de radio multicanal reemplazarán a nuestro actual sistema multicanal de área que es analógico y no se adapta para la trasmisión de datos y otras facilidades de tecnología digital.

i. Terminales de usuarios/suscriptores

Los suscriptores de los ETMU inician y terminan todas las comunicaciones mediante el uso de terminales, entre los cuales se pueden mencionar:

(1) Terminal digital de voz no-seguro, que provee acceso de voz y datos a la red de ETMU. Algunas de sus características principales incluyen: cuentan con auriculares (handset), teclado (Keypad), trasmisión digital a 16 Kbps, cuatro hilos con puerto para datos de interface a computador y/o facsímil, compatible con otros terminales.

(2) Terminal digital de voz seguro, que provee acceso de voz y datos seguro a la red de ETMU. Sus características son similares al anterior.

(3) Facsímil, que trasmite en segundos sobre el sistema, info crítica tales como calcos, diagramas y mensajes escritos a mano. Sus características están estandarizadas para versiones de 16 Kbps.

j. Conmutadores de entrada de la fuerza (CEF)

(1) Los CEF combinan las funciones esenciales de las cabinas de los CCN, ENG y las facilidades de administración de nodos y una UAR en una sola cabina; que al combinarse con los radios multicanal de solo banda UHF comprimen el paquete de comunicaciones contingentes. Las conexiones entre los CEF y los radios multicanal inicialmente son por cable, desde que no tienen la banda SHF.

(2) Los CEF tienen capacidad de conmutación de paquete, pero no función de gateway; por eso no tiene conexión directa a fuerzas o unidades adyacentes. Algunas de sus características técnicas principales son:

(a) Puede ser operado-controlado fuera de la cabina mediante un terminal remoto de administración de nodo desmontable.
(b) Un conmutador de paquete
(c) Puertos para dos LAN´s y seis X25 locales
(d) Un puerto de discado interno
(e) Interface a radio VHF desmontable
(f) Capacidad de UAR de tamaño reducido hasta para 25 suscriptores.

(3) Los CEF proveen capacidad total de búsqueda por desborde vía un subsistema de enrutamiento de tamaño reducido, capacidad para interfacear con radios de SHF y un terminal digital de voz seguro en la cabina. Una unidad de terminal de línea (LTU: line termination unit) provee funciones de modem/multiplex para interfaces de usuarios locales y está equipado con una tarjeta de terminales posterior para permitir conexiones directas en lugar de caja de interconexiones.

23. ARQUITECTURA DE RED DE LOS ETMU

a. Conforme el Cmdte del EO maniobra a sus GGUUCC, la red de ETMU deberá desplegarse para apoyar a estos elementos. La dirección de la maniobra y la ubicación de los elementos de combate, de apoyo de combate y de apoyo administrativo determinarán la ubicación de las unidades de comunicaciones. El apoyo de ETMU debe ser a los usuarios/suscriptores de la fuerza en todos los escalones, desde el EO hasta los puestos de comando de batallón; pudiendo en algunas ocasiones de acuerdo a la misión, situación, disponibilidad, priorización u otros factores apoyarse a escalones más bajos.

b. La red de ETMU proporciona apoyo de cobertura de área, semejante a una compañía telefónica comercial pequeña; pero con un mixtura de equipos alambricos e inhalámbricos, seguros o no y con capacidad de proporcionar el apoyo en movimiento. Este última capacidad se provee tanto con los terminales radiotelefónicos de usuario móvil (TRUM) como con una interface especial a red de radio segura para los equipos de radio monocanal de combate (CNR-900 y/o HF-2000 por ejemplo).

c. Los conmutadores de centros nodales (CCN´s) son dispuestos desde la zona de retaguardia del EO hasta el límite anterior de la zona de las GGUU en base a factores geográficos (área de cobertura) y densidad de usuarios/suscriptores (cantidad de personas/unidades/lugares por enlazarse o interconectarse). Los CN´s se despliegan de manera algo independientemente a la existente estructura de comando y normalmente no todos serán comprometidos al mismo tiempo; lo que dará al sistema de control (SISCON) la flexibilidad necesaria para cambiar ETMU que enfrenten la misión operacional.

d. Como se ha manifestado, una unidad de comunicaciones que apoya a un EO de hasta cinco GGUUCC puede desplegar hasta 16 centros nodales; y cada unidad de comunicaciones que apoye a una GUC de hasta cuatro batallones de maniobra y tres unidades de apoyo de combate y una unidad de apoyo administrativo, como elementos constitutivos básicos, podrá desplegar hasta 5 centros nodales. Cada CN debe conectarse a por los menos otros 3 CN´s para proporcionar rutas de enlace redundantes que supervivan a probables interrupciones por efectos de acción enemiga. Toda esta arquitectura formaría así una red malla backbone.

e. En la figura 1, se muestra un ejemplo de arquitectura de ETMU dividida en tres capas. La capa superior es una estructura backbone que consiste de CN´s interconectados; la capa inferior consiste de usuarios/suscriptores móviles y estáticos (conectados con cable/alambre). Dependiendo de la cantidad de unidades por apoyar, el equipamiento de ETMU disponible y otros factores; en una Z/O de un EO pudieran desplegarse más de 200 ENP´s y más hasta 9 ENG´s; ya que los ENP´s pueden apoyar a puestos de comando desde el escalón batallón. Por otro lado, como se aprecia en la figura las unidades de acceso radial también proveen apoyo a usuarios/suscriptores móviles pudiendo haber hasta 60 UAR(8 en cada GU y 20 en el EO) apoyando cada una entre 20 a 25 suscriptores.

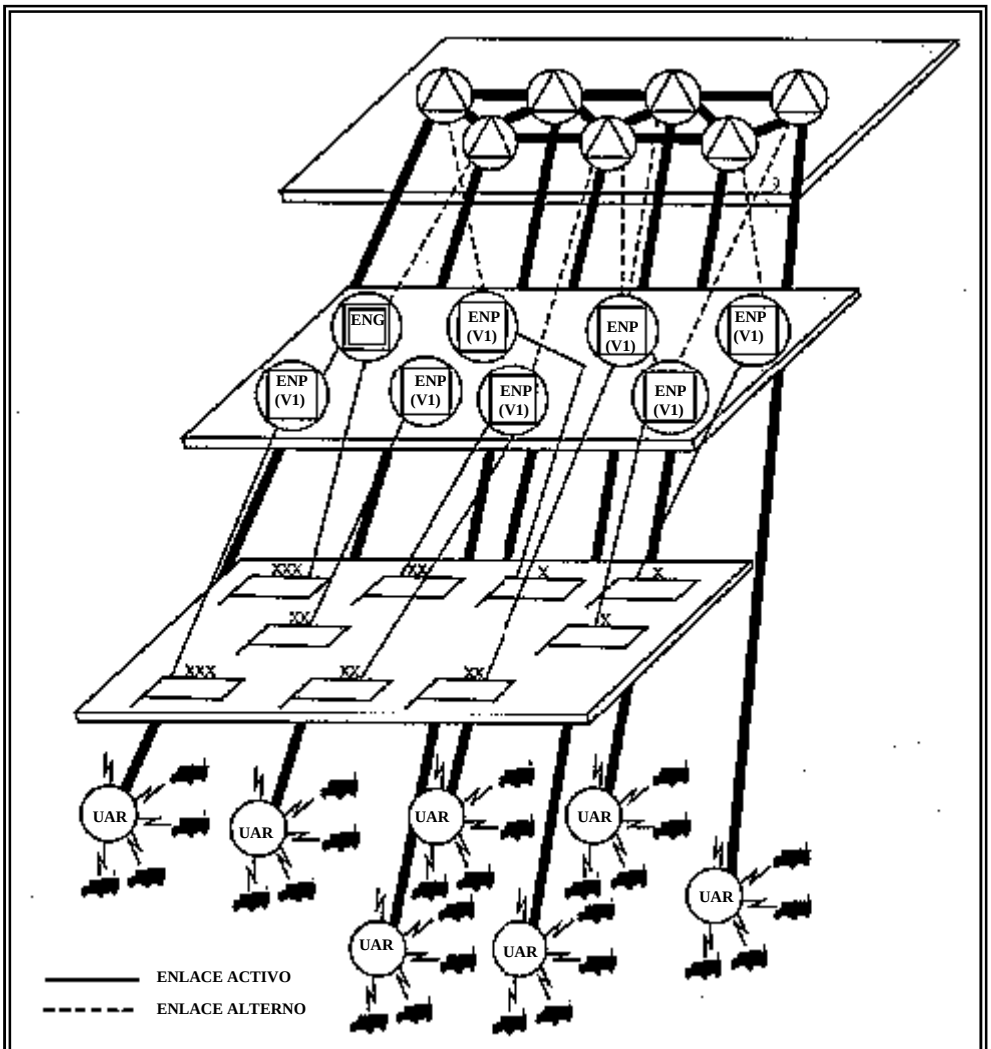


FIGURA 01: ARQUITECTURA DE ETMU

24. IMPACTOS DE LOS ETMU EN EL EJERCITO

a. Impactos doctrinarios

(1) La introducción de la tecnología de ETMU van a variar sustancialmente la forma como tradicionalmente los comunicantes satisfacían las necesidades de enlace de sus cmdtes y diversos elementos apoyados. Igualmente van a permitir a los cmdtes de las unidades de maniobra ejercer el C^2 de sus fuerzas en casi todo momento, en tiempo casi real y desde el movimiento, con menor necesidad de mensajes de voz, reducido empleo de estaciones de control de redes radiales, amplia capacidad de conmutación e integración radio-alambrica hasta al nivel soldado inclusive en caso necesario.

(2) Por ejemplo el desplazamiento de los puestos de comando no será ya más un problema de riesgo de perdida de enlace, ya que los ETMU proveen comunicaciones continuas y en profundidad durante el movimiento de las fuerzas y de los PPCC. Igualmente los tiempos de instalación de sistemas alambricos se reducen, con el empleo del cable troncal y enlaces radiales SHF; así como la búsqueda de rutas por desborde aseguran la supervivencia de la red a pesar del daño por acción enemiga o desperfectos del equipo, sobrecarga en el flujo de información o cambios constantes de ubicaciones de los suscriptores/usuarios.

(3) Los ETMU permiten una posibilidad que antes no contabamos, que es la de conmutación automática dentro de la Z/O en cualquier parte que el cmdte o algún elemento designado se encuentren, aún cuando la unidad de comunicaciones que lo apoye pueda no tener capacidad para procesar la llamada de su cmdte hacia algún elemento con quien él desee enlazarse, pues la red malla encontrará alguna ruta buscando la dirección única asignada a ese elemento para toda la red.

(4) La administración centralizada de la red ayudará al cmdte de la unidad de comunicaciones que apoya al EO, a mantener el control técnico sobre todos los recursos de comunicaciones dentro de la Z/O. Sin embargo deberá desarrollarse para la red del EO estándares operativos técnicos uniformes a través de procedimientos operativos vigentes (POV´s) efectivos. Se requerirá de una relación de trabajo sólida entre los G-6´s y cmdtes de unidades de comunicaciones de todos los escalones para ser exitosos en el apoyo de Telemática.

(5) Las interconexiones de redes del EO y las GGUUC que la integran serán más precisas, eficientes y de mayor cobertura; facilitando el despliegue de las fuerzas sin la perdida del C^2. Para lo cual los planificadores de Telemática (G-6´s y/o cmdtes de unidades de Comunicaciones) deberán visar el despliegue de los recursos de ETMU que apoyen mejor la intención y concepto de opn de sus cmdtes.

(6) La instrucción y el entrenamiento del personal de comunicaciones será crucial; pero más crítico aún será la educación de los usuarios que no son comunicantes, particularmente en los escalones de batallón donde el S-6 u Oficial de comunicaciones cobra dentro de esta nueva tecnología mayor relevancia, ya que ellos realizarán funciones críticas para los administradores de red de Telemática tales como:

(a) Entrenar a los usuarios de los equipos de comunicaciones

(b) Definir las necesidades de sus cmdtes y elementos de su unidad

(c) Coordinar detalladamente los requerimientos de comunicaciones y datos de la unidad.
(d) Identificar con exactitud los problemas de los usuarios/suscriptores.
(e) Asegurar la coordinación de esfuerzos para solucionar problemas
(f) Coordinar inmediatamente cualquier salto de cambio de ubicaciones.

b. Impactos técnicos
(1) Dentro del sistema de ETMU, el hardware y el software determinarán el enrutamiento de las llamadas, la capacidad de conmutar troncales y las características de señalización. Esto permitirá a los planificadores de Telemática administrar más recursos, y solo en casos especiales en que los gateways no pertenecen al sistema de ETMU los planificadores tendrán que tomar decisiones respecto al enrutamiento y demás características.
(2) La capacidad de enrutamiento automático de llamadas buscando rutas de desborde sobre enlaces óptimos en una básica llamada por llamada entre dos puntos terminales dentro del área de cobertura, omitirá la necesidad de contar con tablas de conmutación de rutas; ya que la llamada será direccionada de centro nodad a centro nodal hasta llegar a la dirección (código o número asignado) buscada.
(3) Existen otra serie de impactos técnicos que mejorarán el rendimiento técnico de las redes de comunicaciones de todos los medios; pero al mismo tiempo impondrán un reto a los oficiales, técnicos y suboficiales de comunicaciones, por tener y alcanzar una mejor capacitación y entrenamiento para ser eficientes en la operación de esta nueva tecnología.

c. Impactos en las organizaciones de comunicaciones
(1) Las actuales organizaciones (unidades) de comunicaciones deberán ser reestructuradas y dimensionadas de acuerdo a la nueva tecnología con elementos más flexibles, modulares y altamente capacitados para operar este sistema.
(2) Estas nuevas organizaciones deberán también estar adaptadas para intervenir desde época de paz, para apoyar a la defensa civil en casos de desastres naturales en cualquier lugar del territorio nacional donde una de las consecuencias de dichos desastres es la perdida o quiebre de la infraestructura de comunicaciones (falta de energía eléctrica, caída de torres de retrasmisión, corte o rotura de líneas físicas o de cable/fibra, etc). En tales circunstancias los ETMU se constituyen en una magnífica alternativa para restablecer y mantener comunicados a la zona o área de desastre, proporcionando enlaces para los comandos respectivos, sectores o dependencias de ayuda humanitaria, hospitales y hasta organismos no gubernamentales nacionales o internacionales.

SECCION III. SISTEMA DE REDES RADIO MONOCANAL DE COMBATE (SRMC)

25. INTRODUCCION A LOS ETMU

a. Las redes radiales de combates son aquellas que se establecen o forman alrededor de funciones específicas dentro de una zona de batalla; tales como operaciones, inteligencia, logística-personal, etc; que contiene grupos específicos de usuarios dentro de una GU o unidad.

b. Las ventajas de una red radial de combate, con respecto a otras redes de medios, son su fácil instalación y alta movilidad; que le permite apoyar como medio principal de comunicaciones de voz para enlaces internos a las unidades de escalón GU y menores, en especial durante los desplazamiento y las maniobras de combate y/o de apoyo de combate.

26. FORMAS DE EXTENDER EL ALCANCE DE LAS REDES RADIALES

a. Para sobrepasar los obstáculos del terreno o establecer el enlace entre estaciones bastante alejadas (más allá de 30 Km aproximadamente), se emplean sistemas de extensión del alcance; los cuales serán necesarios para algunos tipos de unidades, de misión o de terreno.

b. Estos sistemas de extensión incluyen radio mono o multicanal con equipos de inserción, integración y/o de retrasmisión en VHF/UHF/SHF, radios de HF, estaciones satelitales o cualesquiera de otros métodos tales como amplificadores de potencia, antenas de alta ganancia, etc.

c. El G-6/S-6 será responsable por el planeamiento y preparación de equipos de retrasmisión/radiorelevadores, que serán empleados sobre todo el campo de batalla, en especial para asegurar que se les provea responsable el Cmdte de la U/Com.

d. Algunos de los factores claves que facilitarán el éxito del empleo de los sistemas de extensión de alcance son:

(1) Integración y sincronización de las actividades sobre el campo de batalla (Ver párr 8,planeamiento de un Cmdo de Telemática, apéndice G, Anexo 3 del ME 11-30 Ed 1999)

(2) Realización del análisis de riesgos con opciones lógicos y posibles en la elección de emplazamientos y rutas de desplazamientos (Ver Anexo 5 del ME 11-30 Ed. 1999).

(3) Análisis y uso del terreno. Ambos parámetros serán importantes cuando de supervivencia, sostenimiento y accesibilidad cuando se planeen los emplazamientos.

27. ESTRUCTURA DEL SISTEMA DE REDES RADIALES MONOCANAL DE COMBATE

a. La estructura del sistema de una red radial monocanal dependerá de la situación existente, concepto inicial del Cmdte, tipos de equipos orgánicos y disponibilidad de los mismos. Actualmente las redes radiales están diseñadas alrededor de tres sistemas de radio separados, los cuales tienen diferentes capacidades y características de trasmisión. Estos sistemas son:

(1) Sistema de redes de radio monocanal VHF-FM (tierra-tierra, tierra-aire-tierra).

(2) Sistema de redes de radio monocanal HF mejorado.

(3) Sistema de redes de terminales satelitales tácticos monocanal (comercial/militar)

b. El principal rol del SRMC es la trasmisión de voz para el C^2 de la GU/Unidad, pero puede asumir un rol secundario para la trasmisión de datos exceden las capacidades de los equipos terminales móviles de usuario (ETMU) o del sistema de distribución de datos del ejército. La trasmisión de voz tendrán prioridad sobre la trasmsión de datos en muchas redes, pudiendo ser al contrario en las redes de apoyo de fuego y defensa aérea para datos de reglaje, dirección del tiro, etc.

28. SUPERVISIÓN DE LA ESTRUCTURA DEL SRMC

El G-6/S-6 será responsable por asegurar que los usuarios conozcan como operar los equipos de radio como un sistema dentro de las redes; para lo cual:

a. Asegurarán que el personal de la GU/Unidad sean eficientes en la operación de los equipos.
b. Asegurarán que todos los operadores de radio de la GU/Unidad estén familiarizados con los procedimientos de explotación radioeléctricos de las redes, planes anti-perturbación, medidas de seguridad de trasmisión y operaciones de retrasmisión en los sistemas VHF-FM.
c. Monitorean la disciplina de red y hacen las correcciones que sean necesarias.

29. TIPOS O CATEGORIAS GENERALES DE REDES RADIALES

a. Sistema de redes radio VHF-FM.- Las unidades desde los escalones, compañías independientes hasta el EO inclusive, normalmente deberán establecer las siguientes categorías de redes:
   (1) Redes de comando y control
      (a) Estas redes a su vez se subdividen en las redes funcionales siguientes:
         1. Redes de Unidades de maniobra (operaciones).
         2. Redes de Unidades de apoyo de fuego.
         3. Redes de Unidades de defensa aérea.
         4. Redes de Unidades de apoyo aéreo
         5. Redes de Unidades de supervivencia y movilidad (ingenieros).
      (b) Estas unidades establecen sus redes internas de C^2 y serán suscriptores en la menos una u otra red. En este manual, las redes mostradas sólo sirven como una guía, ya que como se ha manifestado la estructura final del sistema a establecerse dependerá de la situación existente, orientación del Cmdte y equipo disponible, entre otros factores.
   (2) Redes de apoyo logístico/personal
      Las unidades establecen estas redes de acuerdo a sus necesidades; sin embargo es conveniente que todos los escalones tengan una red de apoyo separada para la información operacional; para prevenir que la red de C^2 sean sobrecargada durante el combate/batalla.
   (3) Redes de Inteligencia/reconocimiento inmediato
      Estas redes usualmente se establecen desde el nivel batallón hasta división para pasar información de manera continua, por lo que requerirá que sea separada de las redes de C^2 para impedir la sobrecarga de estas últimas. La situación local determinará si otros suscriptores serán agregados o retirados.

(4) Red de Cmdo de batalla de retaguardia/Reserva
Esta es una red clave que consiste en el enlace con las unidades co-localizadas en la retaguardia, para dar seguridad al área de servicios, zonas críticas o que están como reserva.

b. Sistemas de redes de radio de HF mejorado.- Las redes de radio HF son similares a las redes de VHF-FM en función y estructura. Muchas redes de HF son complementarias o para doblar a las de VHF-FM y se establecen cuando la dispersión de la unidad excede el alcance de planeamiento para los sistemas de VHF. Las redes que normalmente se establecen en HF son:

(1) Redes C^2 en HF
Se establecen como un medio secundario de control de batalla y para doblar a las redes de C^2 en VHF. Cuenta con los mismos tipos de redes funcionales que en VHF y será la red de reserva que se empleará cuando la dispersión de las unidades de la GU/EO extiendan la línea de comunicaciones; pero deberán ser reemplazadas tan pronto como sea posible por el sistema de comunicaciones de área de usuario común.

(2) Redes de C^2 de unidades logísticas en HF
Las unidades logísticas usan las radios de HF para el C^2 y coordinación interna debido a las distancias de comunicaciones entre áreas de servicio. Las unidades de apoyo dentro de un EO establecerán redes similares o monitorearán las redes de la división para asegurar el apoyo hacia delante.

(3) Redes de reconocimiento y de unidades de caballería
Los reconocimientos y las unidades de caballería requieren de radio HF para proveerse de comunicaciones de largo alcance con sus patrullas de reconocimiento. Los regimientos, escuadrones de caballería y las tropas usarán baja potencia de HF para sus redes de C^2.

(4) Redes de apoyo médico especializado
Las unidades médicas especializadas (UQM, hospitales de campa, etc) requerirán de sistemas de comunicaciones dedicados, de largo alcance y confiables para apoyar a los puestos de socorro, sistema de evacuación y en el tratamiento en el movimiento. Para ello se necesitará contar con equipos de HF que cuenten con sintonía automática de botón-presionado y otras características de simplificación de operación, que permitan que personal que no sea de comunicaciones puedan operarlo.

(5) Redes de Unidades de Fuerzas Especiales
Las unidades de Fuerzas Especiales por el tipo de misión que realizan requieren equipamiento a nivel patrulla a grandes distancias, con transmisiones en Datos en Salto de Frecuencia en HF, siendo así confiable, seguro , y anti guerra electrónica.

c. Sistema de redes terminales satelitales tácticos monocanal

(1) El manual de empleo de las comunicaciones satelitales en el ejército (ME11-70) describe ampliamente la teoría y técnica de los equipos satelitales comerciales y algunos militares. En este manual se propone como los recursos satelitales (comerciales y militares) podrían emplearse en red, cuando son del tipo monocanal.

(2) Por la característica de trasmisión de este sistema y debido a que el ejército, ni tampoco el estado peruano cuenta con satélite propio, el

empleo de redes de terminales satelitales deberá realizarse adoptándose las máximas medidas de seguridad de trasmisión y para pasar cierto tipo de información para ciertas unidades y/o para cierto tipo de operaciones. Aunque es probable que el ejército o la Fuerza Armada pueda llegar a contar con un transpondedor propio sobre un satélite comercial, los riesgos que las comunicaciones puedan ser interceptadas son altas, por lo que el uso de sistemas de códigos y criptográficos sobre las redes será mandatorio. Por otro lado, el advenimiento de las comunicaciones móviles globales por satélite, han permitido su uso en cualquier parte del territorio nacional, pero siempre dependientes del ambiente de información global.

(3) Existe una alternativa, en la búsqueda de aliados estratégicos con capacidades de contar con satélites militares propios y adquirir sólo los terminales tácticos monocanal y firmar convenios de uso del segmento, esto podría reducir los riesgos contra la seguridad de trasmisión, pero aumenta la dependencia con el aliado.

(4) Por el momento, el reto para el empleo del sistema de redes de terminales satelitales en operaciones militares, será usar los sistemas comerciales con terminales seguros ya sean terminales fijos o móviles-portátiles, monocanal para comunicaciones de largo alcance. Estas comunicaciones deberán ser para informaciones de carácter administrativo no secreto (excepcionalmente para operaciones, inteligencia, apoyo de fuegos, etc) y con normas y procedimientos precisos debido al costo de alquiler del segmento espacial.

(5) Las redes de terminales satelitales será para uso normal en los escalones DE y superiores; eventualmente por razones geográficas o necesidades estratégicas podrían emplearse en escalones menores a los sugeridos.

(6) La configuración de la red dependerá como siempre, de la situación, misión, equipos disponibles, disponibilidades económicas-financieras, etc. De acuerdo a ello, podrían establecerse los tipos de redes siguientes:

(a) Red Satelital de Inteligencia/Operaciones.- Los sistemas de inteligencia del EO, para propósitos de aumentar la velocidad del flujo de informaciones en los canales de comando, pueden establecer este tipo de red siempre y cuando se tengan comunicaciones seguras y dedicadas. El uso de esta red en operaciones estará supeditado a la necesidad de combinar la inteligencia con la info de combate proveniente de los elementos subordinados y de otros comandos adyacentes o de apoyo; para integrar esfuerzos en la preparación de inteligencia del campo de batalla.

(b) Red de Apoyo Administrativo.- Esta red será un medio valioso de apoyo de comunicaciones para ciertas unidades de apoyo administrativo, cuando deban apoyar a las fuerzas dispersas en las zonas de combate y zona de retaguardia; particularmente en la entrada inicial dentro de la estrategia de proyección de la fuerza (Ver Manual de Opns de Info) en que una arquitectura C^4 podría proporcionar conciencia situacional, servicios de multimedia e imagen que le daría la habilidad a dichas unidades de apoyo administrativo para accesar oportunamente material y apoyar el

movimiento de las fuerzas. Esta red satelital así diseñada permitirá principalmente al logístico enfocarse en la disciplina de distribución de recursos en todos los escalones.

(c) Red Satelital de Apoyo de Fuegos.- Esta red será ideal para proveer además de voz, un enlace digital entre los sistemas de artillería automática de datos y los sistemas de observadores avanzados. Adicionalmente podrían ser parte de esta red oficiales de enlace, unidades de caballería en misión de protección o cobertura y todas las UU de artillería del EO, que permitirá coordinar los fuegos cuando estos sean necesarios en un área adyacente a la Z/O que pueda estar controlada por alguien más. Esta coordinación asegurará que dicha área esté bajo control enemigo y no se encuentren tropas amigas en ella.

30. EQUIPOS DEL SISTEMA DE REDES DE RADIO MONOCANAL VHF-FM (SRMC/VHF-FM)

a. Los equipos del SRMC/VHF-FM es el sistema de radio principal empleado para comunicaciones de voz de corto alcance y seguras en los escalones GU y menores y es el medio secundario para las unidades de apoyo de combate y apoyo administrativo.

b. Estos equipos lo constituyen la serie CNR-900, que remplazarán a todas las series AN/PRC-77, AN/VRC-12 y AN/VRC-46 al 49. Los equipos CNR-900 aceptan entradas digital o analógica y puede convertir las Telemática en una salida de modo “salto de frecuencia (FH: frecuency hopping)”, donde las trsmisiones de radio cambian la frecuencia en dos opciones de 100 ó 250 veces por segundo; lo que impedirá o reducirá al mínimo las posibilidades de interceptación y perturbación de los equipos, o de radiolocalización o desorganización de las comunicaciones amigas.

c. Los equipos de CNR-900 tendrán acceso a la red del sistema de comunicaciones de área de usuario común (SCAUC) a través de una interface de red de radio (IRR), que normalmente estará localizada cerca de una extensión de nodo pequeño (ENP), extensión de nodo grande (ENG), conmutador de entrada de la fuerza (CEF) o centro nodal (CN).

d. El principal componente del CNR-900 es el RT-7330, que tiene un circuito interno de seguridad de comunicaciones. Además cuenta con una facilidad de “modo susurro” para evitar hablar en voz alta durante los patrullajes o mientras se está en posición defensiva. El operador susurra en el combinado microtelefónico y será escuchado en el auricular del equipo receptor en voz normal. Dos equipos CNR-900 instalados juntos y con los cables de interconexión apropiados, pueden operar como una estación de retrasmisión.

e. Los equipos CNR-900 tienen las configuraciones siguientes:

(1) AN/PRC-730.- Es una versión portátil a la espalda, cuyo peso es de 8 kgs, con una batería de litio que puede durar 8 horas (en relación de 1 a 9). El alcance de planeamiento de esta configuración es de 5 a 10 km cuando se emplea en la posición High o medium y de 200 a 3 Kms en posición Low.

(2) AN/VRC-745.- Es una versión vehicular cuyo alcance de planeamiento es el mismo que el AN/PRC-730. Sin embargo con amplificador de potencia de 50 watts, su alcance puede estar de 10 a 40 km para fines de planeamiento.

(3) Las dos versiones tienen la capacidad de scanear o monitorear hasta tres canales, más el operativo, dándole una prioridad de ingreso a cada uno. Así mismo es factible por medio del Cable CX 5230 realizar retransmisiones en claro, en secreto o en Salto de Frecuencia con la finalidad de ampliar la cobertura.

f. Como cargar la programación del equipo CNR-900

Este equipo de radio puede ser programado de 4 maneras:

(1) Cargar la programación de la Computadora personal (PC) a la Radio
   (a) Instale el cable CX 5205 entre la PC y RT
   (b) En RT 7330 presione PROG
   (c) Teclee 22222 (si no está programado 29192)
   (d) Presione tecla 2, luego ENT, pantalla LOAD <<<
   (e) En PC, sub menú CNR 900 ingrese SEND DATA, seleccionando RADIO.
   (f) Al terminar carga, lea en pantalla RT LOADED.

(2) Cargar la programación de un G 10 a Radio
   (a) Instale el cable CX 4483
   (b) Pasos "(b), (c) y (d)" del anterior.
   (c) En G 10 presione botón ON, en cuanto apague TEST/END presione SEND
   (d) Espere el final de la carga y lea en pantalla LOADED.

(3) Cargar la programación de Radio a Radio
   (a) Instale cable CX 5230
   (b) En RT que recibe programación paso "(b) del anterior
   (c) En RT que trasmite programación en pantalla PROG, teclee 22222, ENT5, ENT , observe en pantalla LOAD >>>
   (d) Al terminar caga lea en pantalla de equipo que recepciona programación "LOADED".

(4) Programación manual

Los datos a programar son los siguientes:
   (a) Frecuencia fija por canal
   (b) El SCAN
   (c) Número de claves SEC por canal
   (d) Número de parámetros AJ por canal
   (e) Las claves de SEC
   (f) Tablas AJ
   (g) Miscelanias (Tipo SQ, Data SINC/ASINC, Tono ACT/DES, hora, fecha, velocidad AJ)

31. EQUIPOS DEL SISTEMA DE REDES DE RADIO MONOCANAL HF

a. El ejército cuenta con los siguientes equipos de HF
   (1) TRC 372 y TRC 340 (THOMPSON-CSF)
   (2) PRC 2200, VRC 2020 y VRC 2100 (TADIRAN)
   (3) TR 178B y TR 250 (GRINEL)

b. Equipos de Radio Thomsom-CSF

El equipo de radio TRC 372 y TRC 340 son equipos de radio de la generación de los años 70, que no cuentan con medidas de seguridad o salto de frecuencia, sin embargo se han repotenciado para operarlos en la Zona de Emergencia, adaptando el combinado Inteligente HS 154 de GRINEL, que permite distorcionar la voz, logrando dar cierta seguridad en las comunicaciones.

c. Equipos de Radio HF-2000/TADIRAN

Estos equipos de radio se han adquirido en tres versiones:

(1) VRC 2020 (fijo o vehicular).- esta versión fue concebida en su diseño para operar en una GU, pudiendo ser operado a nivel Batallón según la situación requiera.

(2) PRC 2200 (portátil).- puede ser operado para los PPCCAA de las GGUU, así como para algunas Batallones o sus Sub Unidades que lo requiera, de acuerdo a la situación. Tiene un peso de 8 kgs y la batería una duración de 12 horas (relación de 9/1). Las dos versiones mencionadas tienen una potencia de "solo recepción", 5 w, 10w ó 20 w, permitiendo tener un alcance de hasta 3,000 kms.

(3) VRC 2100 (fijo).- esta versión por su potencia de 100 w es de dotación de EO/DE y tiene un alcance ilimitado.

d. Las características operacionales de los equipos HF-2000/Tadiran principales son:

(1) Permite comunicación en seguro (encripción) como parte integral del sistema.

(2) Dispone de Salto de frecuencia de tres tipos:

(a) Salto Manual.- la señal salta de acuerdo a las frecuencias que se programan manualmente. Es posible programar hasta 150 frecuencias, siendo recomendable por las características de propagación de HF, no ingresar más de 30 frecuencias, así como no espaciarlas en más de 2 Mhz.

(b) Salto Secuencial.- dispone de ocho (08) tablas secuenciales y la señal salta de acuerdo a una frecuencia inferior, la cantidad de frecuencias (hasta 150), y el tamaño del paso (la diferencia entre frecuencia adyacentes, Khz, hasta 99 Khz), pudiendo tener hasta cinco (05) frecuencias prohibidas. Así mismo por las características de propagación de HF es recomendable que con la cantidad de frecuencias y el paso no supere el espacio de 2 Mhz.

(c) Salto Central.- la señal salta de manera aleatoria en diferentes frecuencias, alrededor de la frecuencia del canal programado .

(3) Establecimiento automático del enlace con selección de canal libre más silencioso que pueda soportar comunicaciones (función AUTO CALL)

(4) Capacidad de transmisión en "FLASH" para rápidos y breves mensajes numéricos de tres (03) dígitos.

(5) Dispone de dos silenciamientos que acalla la salida de audio cuando no recibe señal útil; uno con codificación digital y otro para compatibilidad con otro equipo de radio HF.

(6) Dispone de un MODEM interno de 50/75/170 baudios sincrónico y asincrónico con para instalar Teletipo (señal de datos de 7 bits).

(7) Dispone de una llamada general, tres grupales y 27 individuales

(8) Dispone de un método de sintonía automático

(9) Se puede programar hasta veintinueve (29) canales

(10) Es factible realizar una INTEGRACIÓN con los equipos CNR 900 con el cable CX 5330.

e. Equipos de radio GRINEL

Los equipos de radio Grinel fueron diseñados y fabricados en su estructura y uso para dotación de unidades de Fuerzas Especiales con características de poco peso, pequeño, fácil de operar y con medidas de COCOME (Salto

de Frecuencia y seguridad simultánea), así como para operaciones en terreno selvático. Se han adquirido en dos versiones:

(1) TR 178B.- Esta versión fue diseñado con fines tácticos hasta nivel patrulla, traduciéndose esto en su tamaño, peso y consumo de batería. Tiene un peso de 4.0 kgs y la duración de la batería es de 12 horas (relación de 9/1). Puede ser alimentado para operarlo en voltajes de 10 a 32 voltios. Dispone de potencia alta (H) de 25w y baja (L) 0.25 W logrando un alcance de hasta 3,000 Km. Cuenta con tres tipos de antenas, la vertical y horizontal conocidas, y una tercera llamada ANTENA TACTICA o CUCARACHA, donde por su diseño la mayor cantidad de señal se desplazan por la ionosfera, permitiendo tener comunicaciones en lugares muy accidentados o en selva (árboles altos) que no permitan instalar una antena horizontal. Dispone de dos tipos de sincronizador, automático y manual. Los sincronizadores automáticos sincroniza cada vez que la máquina lo crea conveniente (se cambia de frecuencia o el medio lo requiera), mientras que el sincronizador manual permite que el operador decida cuando se sincroniza, siendo el manual más recomendable para patrulla que operan en terreno enemigo, a fin de evitar la radiolocalización, conocedores que una calibración es siempre con potencia alta, fácil de detectar. Así mismo disminuya el peso y volumen.

(2) TR 250 (fijo o vehicular).- Esta versión por su potencia de 100 w es de dotación de EO/DE y tiene un alcance ilimitado.

f. Las características operacionales son las siguientes:

(1) El equipo Grinel tiene un dispositivo externo (H 154) para la comunicación en seguridad, pudiendo simultáneamente encontrarse en salto de frecuencia y con la voz en seguridad. Por el diseño para Fuerzas especiales no es recomendable usar solo en seguridad, por que es posible la radiolocalización.

(2) El salto de frecuencia que realiza este equipo de tipo central, es decir realiza saltos de manera aleatoria en un ancho de hasta 1 Mhz alrededor de la frecuencia del canal programado. Es factible seleccionar la cantidad de saltos de cuatro (04) o diez (10) saltos por segundo desde el panel frontal, permitiendo así tener siempre una comunicación en Salto de Frecuencia, aunque las condiciones del medio lo dificulten. Así mismo es factible variar la frecuencia central de salto desde el modo HOPPING (salto de frecuencia), permitiendo evadir cualquier acción de perturbación.

(3) Dispone de Establecimiento automático del enlace con selección de canal libre más silencioso que pueda soportar comunicaciones (función ALE). En la función ALE con tres caracteres alfanuméricos puede identificar a los equipos de radio con posibilidades de llamadas en grupo y sub grupos, con 46,000 direcciones y más de 2,500 combinaciones de grupos y sub grupos.

(4) Capacidad de transmisión de datos con el terminal de datos DT 309, con posibilidad de:

(a) Direccionar los mensajes con un CALSING de tres dígitos alfanuméricos, realizando individuales, grupales o una llamada general.

(b) Alta capacidad de encripción, codificando los mensajes con códigos de ocho (08) caracteres de números, letras y signos o combinación de ellos.
(c) Transmisión en Flash de más de 30 caracteres debidamente cifrados.
(d) Establecer comunicación de PC a PC y de PC a DT empleando el DT 309 como MODEM.

(5) Se puede programar hasta noventinueve (99) canales.
(6) Dispone de un método de sintonía automático en su versión TR250 y TR 178B con el sincronizador AT 241.
(7) Dispone de un MODEM para trasmitir Facsímil de gráficos y textos.

g. INTERCONECTIVIDAD entre los equipos existentes en el Ejército
(1) La interconectividad en fonía en seguridad es posible empleando el combinado inteligente H 154. (Thompson-Grinel).
(2) En Datos es factible empleando el terminal de datos DT 309 como terminal o como MODEM. Como terminal la comunicación se establecería en claro pero con los DATOS CODIFICADOS, dando seguridad para la interceptación y escucha. Empleando el DT 309 como MODEM es factible establecer comunicación en Salto de Frecuencia, encontrándose en la PC en COM 1 un equipo GRINEL y en COM 2 un equipo TADIRAN, con la finalidad de evitar la localización y perturbación. De esa misma manera se podrán integrar los equipos GRINEL y TADIRAN en DATOS con los equipos CNR 900.

32. EQUIPOS DE RADIO PARA ENLACE TIERRA-AIRE

a. El ejército ha adquirido los equipos de radio BENDIXKING. Las versiones que cuenta son las siguientes:
(1) KX – 99 (portatil).- tiene una potencia de 1.5 w con alcance de 100 mts a 3 Kms. Puede dotarse a unidades tácticas o aeronaves para comunicación entre ambas.
(2) KX – 93 A (fijo o vehicular).- tiene una potencia de 20 w con alcance de 3 kms a 50 kms. Es de dotación para aeronaves y estaciones fijas en tierra.

b. Las características operacionales son las siguientes:
(1) Dispone de gama de frecuencias para comunicación radial y para navegación.
(2) Tiene diez (10) canales prefijados.
(3) Cuenta con control de silenciamiento, para ingreso solo de Telemática audibles.
(4) Dispone de escudriñamiento (scaneo) de dos tipos. Uno donde la unidad empezará a escudriñar en las frecuencias almacenadas en la memoria del 0 al 9 y otro donde se escudriña el rango de frecuencias de 25 Khz entre la frecuencia almacenada en la memoria 1 y la memoria 2 (118.00 a 136,975 Mhz como máximo).

SECCION IV. SISTEMA DE DISTRIBUCION DE DATOS DEL EJERCITO (SDDE)

33. ARQUITECTURA DEL SDDE

a. Hasta el momento, en las secciones II y III se ha descrito brevemente parte del diseño de la arquitectura de comunicaciones que apoyan a los sistemas de comando y control, es decir, el sistema de comunicaciones de área de usuario común (SCAUC) principalmente a base de los equipos terminales móviles de usuario (ETMU) y el sistema de redes de radio monocanal de combate (SRMC) principalmente a base de equipos de radio CNR-900 y radios HF 2000 y GRINELL. Otro sistema integrante de esta arquitectura lo constituye el sistema de distribución de datos del ejército (SDDE).

b. El SDDE es parte de un sistema de distribución de datos mayor, que además comprende al sistema de distribución de información táctica conjunta (JTIDS), que no será visto en este manual. El SDDE basa su arquitectura en equipos radiales computarizados que en red constituyen el sistema de reporte de posición / Localización computarizada (EPLRS: Enhanced Position Location System), que proporciona una solución técnica para escalones batallón y superiores, en la satisfacción de sus requerimientos de distribución de datos de los sistemas automatizados del campo de batalla (SAC´s) siguientes:
   (1) Sistema de control de maniobra (SCM)
   (2) Sistema de datos tácticos para la artillería de campaña
   (3) Sistema de control y planeamiento de defensa aérea
   (4) Sistema de análisis de todas las fuentes (inteligencia / guerra electrónica)
   (5) Sistema de control de apoyo administrativo de combate
   (6) Sistema de comando de combate de la división y menores

   Los aspectos conceptuales sobre los SAC´s serán tratados en el capítulo 3, Administración de la automatización.

c. La arquitectura de red del EPLRS debe establecerse para apoyar la trasmisión de C^2, de la conciencia situacional y datos de posición / localización / navegación sobre el espacio de batalla de un campo de batalla moderno; basándose en el concepto de comunidades de EPLRS:
   (1) Una comunidad de EPLRS es aquella que sirve o apoya a la zona de operaciones (Z/O) de una GU y típicamente consiste de estaciones de control de red (ECR) de EPLRS y puestos de radio (PR):
      (a) Una ECR-EPLRS.- Es el elemento de control que se emplea para la inicialización, control y monitoreo de la red del EPLRS; proporcionando administración de red centralizada incluyendo: la asignación de "time slops" a los puestos de radio, el establecimiento y mantenimiento de la sincronización del tiempo para la red, la asignación de los circuitos de control y el control de la transferencia de claves criptográficas. Aunque la ECR-EPLRS principalmente opera con PR´s en su comunidad, también puede intercambiar datos con otras ECR-EPLRS.
      (b) Los puestos de radio (PR´s).-
         1. Son receptores-trasmisores (RT) que proporcionan comunicaciones digitales seguras, resistentes a la perturbación y posibilidades de posición/localización exacta

para los usuarios. Las comunicaciones digitales seguras y resistentes a la perturbación proveen baja probabilidad de interceptación y detección a través de:

a. Salto de frecuencia (512 veces por segundo)
b. Tecnología de espectro expandido (8 frecuencias entre 420 MHz y 450 MHz) incorporados en un modulo de seguridad de comunicaciones.
c. Potencia de salida regulable (desde 0.4 watts hasta 100 watts).

2. Un PR tiene una antena dípolo-omnidireccional, que permite tener alcances de planeamiento entre 3 a 10 kms entre radios, dependiendo de la potencia de salida y del terreno. Adicionalmente cada PR proporciona funciones de retrasmisión que son transparentes al usuario, que dependerán de la distancia máxima que un PR puede cubrir (10 km), asumiendo que existe LDV entre cada radio y que exista suficiente cantidad de radios en los circuitos de enlace (needline):
   a. Una needline será tanto de formato duplex como de formato de grupo-direccionado; y para retrasmisión máximo podrán haber hasta 5 relays (saltos) para duplex y 4 relays para grupo-direccionado cuando se establezca un enlace needline de punto-final a punto-final.
   b. El área de cobertura local para estos tipos de needlines está limitado a dos saltos, que típicamente podrían cubrir el área de un batallón desplegado.
   c. El área de cobertura extendida empleará 4 portadoras de acceso multiple sensible o seis grupos de multifuente y saltos punto a punto, que típicamente podrían cubrir el área desde una GU hasta EO, dependiendo del terreno.
3. Los PR´s están divididos en:
   a. PR´s con base en tierra.- que pueden ser portátiles a la mano/a la espalda, vehiculares y de georeferencia.
   d. PR´s con base en helicópteros
4. Los PR´s proporcionan a la ECR-EPLRS información de tiempo de llegada de trasmisión sobre cada uno y trasmiten/reciben mensajes. Ellos pueden comunicarse entre sí, a través de la ECR, directamente mediante needlines autorizados o por medio de una sub-red local. Los PR´s proveen info de tiempo de llegada y enlaces de mensajes para establecer comunicaciones y hacer el seguimiento preciso, trasmitiendo y recibiendo mensajes hacia y desde la ECR-EPLRS y entre otras PR´s.

(2) Un PR puede comunicarse con otros PR´s o con la ECR-EPLRS dentro de la misma GU o comunidad desde que todas las unidades en ella tendrán la misma clave de tráfico; sin embargo si un PR se mueve dentro de una comunidad adyacente, el control de ella será transferido automáticamente entre estaciones de control de red.

(3) El personal de comunicaciones especialista asignado a una unidad de comunicaciones que apoya a la GU operarán y mantendrán la ECR-

EPLRS, mientras que los puestos de radio (PR) podrán distribuirse a los usuarios de los SOC´s.

34. FUNCIONES PRINCIPALES DEL EPLRS

a. El EPLRS son terminales de computadoras tácticas (TACTER) tipo laptop, a los cuales se les ha adicionado capacidad de comunicaciones y de posición/localización; constituyéndose en un sistema de comunicaciones de estado del arte, de línea de vista y de trasmisión digital radial de sólo datos sobre posición/localización, navegación, identificación y trasmisión de mensajes de texto libre de la unidad o elemento usuario.

b. Posición / localización

(1) El operador del PR ingresa su pedido de posición/localización y recibe en tiempo casi real dicha información actualizada en un formato de código alfanumérico de 10 caracteres que está relacionado a un sistema de cuadrillado de carta militar u otro que esté cargado en el sistema georeferenciado.

(2) Tales datos constantemente están actualizándose y almacenándose en la ECR, y son proporcionados a cada PR cada vez que se solicitan. Adicionalmente, un operador de PR-EPLRS puede solicitar la posición o la visada/alcance de otro PR en la red.

(3) El grado de exactitud de información posicional será dependiente del emplazamiento de la unidad de referencia en la red y de la densidad de PR´s que comprende tal red. Otros factores que pueden afectar la exactitud son: el terreno, las Telemática reflejadas, la difracción de Telemática por multienlaces y la dispersión de las Telemática de radio. Debido a todos estos factores, al menos un 5% de los PR´s desplegados deberían estar referenciados.

c. Navegación

(1) Los corredores de movilidad, las líneas de coordinación, los puntos predesignados (PPD's) o las zonas del campo de batalla (tales como campos minados, zonas de no-fuego, etc) pueden estar especificados en una ECR-EPLRS.

(2) Cuando un usuario autorizado solicita orientación, la ECR-EPLRS trasmite automáticamente un mensaje de alerta al PR cuando éste cruce o ingrese a dichos lugares y se mantiene trasmitiendo mensajes hasta que el usuario salga de dichas áreas, proporcionando datos de visada y alcance para ayudar al operador del PR en la navegación a través de los corredores, líneas y PPD´s (tales como puntos de verificación, marcas terrestres u otras unidades).

d. Identificación

La identificación militar de todos los PR´s en la red serán almacenados en la ECR-EPLRS. Un operador de PR puede solicitar la identificación de un PR desconocido proporcionando las coordenadas del sistema georeferenciado militar de ese PR desconocido o la visada/alcance a ese PR o la ECR-EPLRS. En la ECR-EPLRS, deberá darse la identificación positiva de todos los PR´s en la red, para ayudar al operador de esa ECR en la coordinación de la opn de todos los puestos de radio.

e. Mensajes de texto libre

(1) Los mensajes de texto libre son mensajes cortos que se envían sobre la red de control para comunicarse mediante:

(a) Comunicaciones indirectas de usuario a usuario enrutadas a través de la ECR-EPLRS empleando un artificio de lectura.
(b) Comunicaciones directas de usuario a usuario sobre una sub-red local establecida empleando también un artificio de lectura.

(2) Las siguientes restricciones deberán aplicarse a los mensajes de texto libre:
(a) Máximo 10 caracteres de longitud.
(b) Cualquier PR puede enviar mensajes de texto libre a cualquier otro PR dentro de la misma comunidad de ECR-EPLRS.
(c) No pueden cruzarse mensajes entre GGUU.
(d) El PR sólo puede enviar a un receptor a la vez.

35. DESPLIEGUE DEL EPLRS

a. Un sistema de control (SISCON) asegurará una efectiva administración técnica y operacional del EPLRS, a través de un elemento de la sección S-3 de la unidad de comunicaciones que apoya a la GU, que dirigirá su empleo bajo un diseño de realización de funciones específicas para incrementar la efectividad de las redes de comunicaciones de datos en un ambiente de situaciones tácticas variables.

b. Este SISCON (elemento del S-3) desarrolla un plan de apoyo de Telemática del EPLRS coordinando con los usuarios (SOC´s) y la comunidad de comunicaciones (S-6´s). Este plan será derivado del P/O u O/O de la GU/EO para apoyar la trasmisión de C^2 y datos de la conciencia situacional sobre todo el espacio de batalla.

c. Bajo el concepto de comunidades de EPLRS, un despliegue típico de este sistema podría consistir de hasta 4 comunidades de ECR´s-EPLRS y 4 puertos (para controlar hasta 4 unidades subordinadas), donde cada comunidad podría consistir hasta de 460 puestos de radio de EPLRS.

d. Una sección de EPLRS de la compañía de comunicaciones que apoya a la GU instalará, operará y mantendrá las ECR´s-EPLRS. Adicionalmente tendrá asignados PR´s para realizar funciones específicas que mejoren o suplementen las opns de la red bajo situaciones tácticas variables:

(1) Puede tener hasta 12 PR´s de georeferencia, cuya función principal será proporcionar a la red con buena referencia de la geometría de la unidad para una grabación de posición/localización altamente precisa. Estos PR´s son empleados bajo la dirección del SISCON del elemento del S-3 de la unidad.

(2) Como los recursos de PR´s de georeferencia son insuficientes para proporcionar toda la cobertura que se necesita, el EPLRS debe hacer radiorelevo con otras unidades militares como puntos de georeferencia, en especial con aquellas que requieren precisión en sus opns como son las unidades de artillería e ingeniería. Los PR´s que sirven como relays son controlados por la sección y se emplean en áreas donde los usuarios de PR´s pudieran estar separados por el terreno, mejorando la conectividad de la red.

(3) Los puertos (gateways) permiten un enlace de comunicaciones entre múltiples comunidades de ECR-EPLRS. Cada comunidad múltiple tiene su propio tiempo de sincronización y claves criptográficas que no permite la continuidad de operaciones con otras comunidades múltiples, por lo que los gateways permitirán las comunicaciones de datos entre estas comunidades (o entre GGUU).

36. CAPACIDADES OPERACIONALES IMPORTANTES DEL EPLRS

a. Capacidad y rendimiento máximo absoluto
   (1) Esto sólo se podrá alcanzar bajo condiciones ideales, limitados sólo por el hardware del sistema, tales como máxima velocidad a la cual pueden enviarse los mensajes fuera de la ECR o la máxima cantidad de mensajes de unidades que la ECR puede almacenar en base a las limitaciones del tamaño de su memoria.
   (2) Por ejemplo, la cantidad de mensajes de unidades activas (PR´s) por ECR está limitado a no más de 470 PR´s.

b. Capacidad y rendimiento máximo práctico
   (1) Estas capacidades están basadas en condiciones que normalmente se presentan en una Z/O donde el clima, las condiciones atmosféricas, pérdidas/restricciones operativas, y el terreno afectarán el rendimiento del EPLRS.
   (2) Por ejemplo, cuando una ECR envía un mensaje, pudiera suceder que el PR no siempre recibirá este mensaje debido a interferencias, ruidos u otros factores.

c. Capacidades de comunicaciones
   (1) Al nivel de red, la capacidad de comunicación estará definida en términos de rendimiento y será dependiente del número de PR´s en la red. Por ejemplo, si una comunidad tiene 250 PR´s de EPLRS con una distribución de recursos de 25% para necesidades de comunicaciones de formato de grupo-direccionado y 75% para necesidades de comunicaciones de formato duplex; entonces esta comunidad tendrá una capacidad máxima práctica de 300 kbps en apoyo a circuitos duplex y de 450 kbps en apoyo a circuitos de grupo-direccionado.
   (2) Al nivel PR, la capacidad del PR y de la needline estarán definidas por el rendimiento más alto que ellos puedan tener en una red manejable. El tiempo disponible será un factor limitante en la capacidad de needline, que individualmente puede apoyar la transferencia de datos en formato de grupo-direccionado hasta 3,840 bps y en formato duplex hasta 1920 bps para cobertura local; y, hasta 56,600 bps para cobertura extendida.
   (3) Los PR´s apoyan múltiples needlines simultáneamente (hasta un máximo de 32), dependiendo de la ubicación de los timeslop lógicos asignados a comunicaciones duplex o grupo-direccionado.

d. Capacidades y rendimiento del control de red
   (1) La ECR usa al control de red del EPLRS para enviar comandos, mensajes, respuestas de posición/navegación y mensajes de texto libre a los puestos de radio. También es empleado para recibir reportes (situación, fallas de needline y reportes de tiempo de llegada) y mensajes (pedidos o solicitud de posición/navegación y mensajes de texto libre) desde puestos de radio.
   (2) El rendimiento y capacidad del control de red está principalmente limitado por:
      (a) Que tan rápido la ECR puede enviar mensajes a los PR´s.
      (b) Capacidad de almacenamiento disponible en la ECR y en el PR.
      (c) Exactitud de las medidas de tiempo de llegada.

37. TERMINAL TACTICO (TACTER)

a. El ejército del Perú aún no cuenta con el sistema de reporte de posición / localización computarizada (EPLRS) descrito brevemente en los párrafos 33 al 36 de esta sección; sin embargo ha iniciado la adquisición de terminales tácticos (TACTER) de procedencia Israelí, los cuales con arreglos especiales, integraciones apropiadas y software especialmente diseñados se pueden desarrollar sistemas pequeños de posición/localización automática.

b. El Terminal Táctico es una computadora compatible IBM-PC/AT Pentium que incluye un GPS incorporado, contiene una memoria RAM de 16 MB y un disco de 340 MB. Dispone de dos (2) entradas para canal 1 y 2 de comunicaciones tácticas. En su software contiene el programa SCOUT para trasmitir y recibir mensajes y el programa NEGEV de cartografía que dispone un mapa digitalizado con la finalidad de navegar con ayuda del GPS.

c. El programa NEGEV permite trasmitir la posición cuando sea solicitada por medio de los equipos CNR 900. Así mismo se puede programar que trasmita de tiempo en tiempo la mencionada posición, siendo trasparente al operador esta trasmisión; permitiendo funcionar como un sistema de reporte de posición/localización computarizada (EPLRS), cuando se requiera o de manera eventual.

d. Mayor información sobre los TACTER se desarrollará en un manual técnico especial.

SECCION V. INTERNET TACTICA (IT)

38. CONCEPTO DE INTERNET TACTICA (IT)

a. La IT es la integración de radios monocanal tácticos, computadoras y equipos de comunicaciones de apoyo, dentro de una red móvil de comunicaciones tácticas de voz y datos; para proporcionar a los combatientes la habilidad para accesar a la red de información del combatiente (ver sección II, Cap 7 del ME 11-70, Empleo de comunicaciones satelitales) con el sistema de comando de batalla de ejército (SCBE) (ver párrafo 17 de este manual), en cualquier ubicación y/o en movimiento (ver sec. I cap. 7 del ME 11-70); enviando o recibiendo automáticamente, información en apoyo a las necesidades operacionales de enlace y a las organizaciones de tarea en la ejecución de sus operaciones tácticas. LA IT es considerada una red WAN.

b. La IT es básicamente una red de comunicaciones automática basada en ruteadores que emplea protocolos estándares de internet comercial para transmitir los datos vertical y horizontalmente sobre una zona de operaciones y hacia otros escalones empleando un paquete de red táctico del equipo terminal móvil de usuario (PRT/ETMU). Las herramientas de administración de red automatizados en los diferentes escalones proporcionarán capacidades de planeamiento, monitoreo y reconfiguración.

39. LA INTERNET TACTICA Y EL SCBE

a. Aunque el SCBE, en particular el sistema de comando y control táctico del ejército (SC2TE) no son parte de la IT; será sin embargo su principal

usuario ya que le permitirá mejorar su habilidad para C^2 convirtiendo a esta habilidad en un multiplicador significativo de la potencia combativa.

b. El G-6/S-6 y el cmdte de la unidad de comunicaciones que apoyan a la GU/EO, planearán y proveerán respectivamente, los enlaces de comunicaciones sobre los cuales se intercambiarán informaciones de comando de batalla dentro de un gran ambiente operacional del SCBE.

c. Los seis (06) sistemas operacionales del campo de batalla (SOC's) mencionados a lo largo de este manual y que son componentes de la disciplina de administración de la automatización (ver capitulo 3), proporcionarán información situacional y apoyo a la toma de decisión, cuando estén integrados dentro de una internet táctica.

40. COMPONENTES DE COMUNICACIONES QUE APOYAN A LA IT Y AL SCBE

a. Los principales componentes de comunicaciones que apoyan a la IT y al SCBE son:
   (1) Sistema de reporte de posición/localización computarizado (ELPRS)
   (2) Sistema de redes de radio monocanal VHF-FM mejorados.
   (3) Sistema de comunicaciones de área de usuario común con ETMU mejorado.
   (4) Terminales de radio digial de aproximación/integración.

b. La IT esta integrado con el SCBE total a través de un interface en el centro de operaciones táctico del EO (COTEO) o en el PC principal de una GU, mejorando la satisfacción de necesidades de información en todos los escalones. La funcionalidad de la IT esta en el desarrollo de redes de área local (LAN's) para los diferentes puestos de comando de todos los escalones que se interconectan entre sí para conformar una red de área amplia (WAN).

c. La interconexión de las LAN's a través de gateways o enrutadores, posibilitarán el flujo de información entre el nivel de plataforma del escalón más bajo (incluso a nivel soldado/individuo) hasta el escalón EO y sobre todo el SCBE.

d. La red de terminales de radio digital de aproximación/integración establecerá el enlace de la IT a todos los puestos de comando (PPCC) del SCBE, proporcionando o constituyéndose en el principal sistema de trasmisión de datos inhalámbrico.

41. ARQUITECTURA DE LA IT

a. La arquitectura de la IT consiste de sub-arquitecturas de C^2 y de conciencia situacional que proporciona intercambio de datos de C^2 e información de conciencia situacional (localizaciones amigas y enemigas) respectivamente. Estas sub-arquitecturas también proporcionan un medio para la trasmisión de voz segura y pueden operar simultáneamente cuando la plataforma esta puesta para voz y dato, de una manera transparente al usuario.

b. Los sistemas componentes mayores que constituyen la arquitctura de la IT son:
   (1) El sistema de comando de combate de división y menores (SCCDM).
   (2) ELPRS
   (3) Terminales de radio digital de aproximación/integración.
   (4) Sistema de redes de radio monocanal VHF-FM mejorados.

(5) ETMU mejorado.
(6) Receptores GPS.
(7) Servicio de difusión global (SDG).
(8) Vehículo del G-6/S-6
(9) Router gateway
(10) Conmutadores de internet LAN.
(11) Plataformas de C^2
(12) Servidor

c. Todos estos componentes serán desarrollados con mayor amplitud en un manual especial de internet táctica, sin embargo algunos de ellos ya han sido sucintamente vistos a lo largo de estos dos primeros capitulos, por lo que en los párrafos subsiguientes se ampliarán conceptos de algunos componentes en su relación con la IT.

42. LA INTERNET TACTICA EN EL SCCDM

a. El ME 11-70 (empleo de las comunicaciones sateitales) en su capitulo 7, sec. II, hace una introducción a la Red de información del combatiente , en el ME 11-30 (organización y operaciones de EM de Com) en su anexo 3/apéndice G, se hace una introducción al sistema de C^2 táctico del ejército, en el ME 11-13 (opns de info) en su cap. 5, de detallan los sistemas de información, dentro de los cuales se encuentra el SCCDM (párr 57.c.(2)) y en este manual en su párrafo 17 se amplían los conceptos que relacionan los sistemas de Comunicaciones con los sistemas de información.

b. La internet táctica es la principal arquitectura de comunicaciones que apoya al combatiente en los escalones GU y menores, mejorando la forma de compartir los datos de C^2 por los Cmdtes, los EEMM, las unidades, las tropas y las plataformas de armas; así como la letalidad de la fuerza, el ritmo operacional y la supervivencia, mientras proporciona conciencia situacional en tiempo casi real. La IT consiste de ruteadores, EPLRS, SRMC mejorado y otros equipos de comunicaciones que usan protocolos estándares de internet comercial para transmitir datos vertical y horizontalmente sobre toda la zona de opns de una GU/EO. El sistema de control integrado (SISCONI) proporciona las capacidades de planeamiento, monitoreo y reconfiguración de la IT.

c. El SCCDM intercambia info con los otros componentes del SCBE, incluyendo aquellos instalados en plataformas de sistemas de C^2 tales como: el vehículo de cmdo de batalla, el vehículo de C^2 y el sistema de C^2 helitransportado. Este intercambio consiste de mensajes seleccionados e interoperables de "formato de mensaje variable conjunto (FMVC)". Para este intercambio se emplea un arreglo de hardware y software que proporcionan conciencia situacional sobre el movimiento, en tiempo real y tiempo casi real, así como info de C^2 para el Cbte, apy de cbte y apy administrativo desde el PC/GU hacia los elementos subordinados. Un computador "host" emplea software de C^2 y enlaces a una red mediante los sistemas de radio táctico.

d. Aunque la IT apoya principalmente a los escalones GU y menores, el cmdte de la unidad de comunicaciones que apoya al EO y el G-6 del EO desempeñarán funciones importantes para la opn exitosa de la IT, por lo que deberá existir una relación de trabajo estrecha entre los G-6's/S-6's de todos los escalones para asegurarse que se están satisfaciendo las

necesidades de los usuarios y que se están distribuyendo apropiadamente los recursos de comunicaciones. Desde que la IT se enlaza al SCBE, el G-6 del EO deberá asegurarse que exista una adecuada administración de las redes LAN's dentro del COTEO y puestos de comando táctico de las GGUU/unidades, así como que el sistema de comunicaciones de área de usuario común (SCANC) provea una adecuada WAN vía el ETMU para apoyar al flujo de info de la IT. El G-6/GU por su parte planeará, monitoreará y cambiará funcionalmente la IT para apoyar al esquema de maniobra del cmdte de la GU, para lo cual mantendrá una estrecha coordinación con los S-6's de los batallones orgánicos, asignados y/o de refuerzo de la GU. Finalmente los S-6's de las unidades asesorán sus Cmdtes y demás miembros del EM en el empleo y operación de la IT, interactuando principalmente con el S-3 de la unidad y tomando parte activa en el planeamiento.

e. Los especialistas para manejar todo el sistema de IT (funciones de inicialización y/o reinicialización) se ubicarán en la unidad de comunicaciones que apoya a la GU. Ellos además tendrán la responsabilidad del mantenimiento y evacuación, de los equipos digitales defectuosas para su manto de A/D para su reemplazo o reparación. Estos especialistas coordinan estrechamente con el G-6, quién deberá contar con un vehículo que transporta una cabina tipo S-250 que contenga todas las facilidades para el planeamiento, la configuración y la administración de la IT y que además sirva como plataforma de integración con las capacidades para hacer el interface de la IT con los ETMU/SCAUV.

f. El vehículo del G-6 se ubicará cerca al PC principal de la GU y contendrá además del computador "host" con los equipos siguientes:
   (1) Equipos VHF-FM con controlador de internet.
   (2) Interfaces X25 para el paquete de red táctico del ETMU (PRT/ETMU)
   (3) Interfaces para terminales de radio digital de aprox/integración, LAN/PC.
   (4) EPLRS
   (5) Estaciones de trabajo (workstation) necesarios de acuerdo a la configuración.

43. LA INTERNET TACTICA EN EL EPLRS

a. El empleo del EPLPS en la IT provee apoyo óptimo al cmdte al permitirle mejorar su habilidad para administrar el tiempo y controlar el ritmo, reduciendo niveles de EM y realizando un mejor intercambio, análisis y procesamiento de informaciones.

b. La administración de la red, a través de la IT, apoyará las funciones críticas del EPLRS siguientes:
   (1) Establecimiento y mantenimiento automático del control de red.
   (2) Establecimiento y mantenimiento automático de la red de comunicaciones:
      (a) Adaptación a la conectividad limite debido al enmascaramiento del terreno
      (b) Adaptación a los cambios de conectividad debido al movimiento de los usuarios y perturbadores enos.
      (c) Establecimiento de enlaces needline usando relays como sea necesario.
      (d) Administración de la seguridad de la red.

(3) Determinación y reporte de posición/localización .
(4) Distribución de la identificación de unidades amigas
(5) Apoyo a las funciones de C^2
(6) Orientación sobre los corredores de movilidad
(7) Penetración en límites.
(8) Monitoreo del rendimiento del sistema.

44. LA INTERNET TACTICAS EN LOS TERMINALES DE RADIO DIGITAL DE APROXIMACION

a. Los terminales de radio digital de aproximación/integración (TRDA) son radios de última generación que operan en la banda de UHF (225-450 Mhz) en pasos de sintonía discreta de 0.625 Mhz, para trasmitir y recibir datos encriptados, protegidos con FEC (foward error correction), códigos de detección y modulados sobre un portador de radiofrecuencia. Su rendimiento digital nominal es de 200 Kbps
b. Los TRDA soportan las interfaces LAN (Ethernet) y seriales (RS-423 asincrónica y RS-422 sincrónica/asincrónica), con un alcance de 10 a 20 Kms. Tiene incorporado capacidades de GPS que proporcionan la posición del radio.
c. Los TRDA son el principal sistema de trasmisión de comunicaciones de datos que enlaza al SCBE a los escalones GU y menores, proporcionando una red inhalámbrica WAN a los combatientes que empleen sus computadores host del SCBE ubicadas en sus PPCC, para la trasmisión de datos a velocidades altas y para el flujo de info de imágenes y datos C^2. Estos equipos se emplean en las plataformas siguientes: vehículo de cmdo de batalla, vehículo de C^2 y sistema de C^2 helitransportado.
d. El G-6/GU establecerá las redes de los TRDA que apoyarán al P/O de la GU, para lo cual establecerá grupos de redes separadas y una red backbone que los conecte. El enrutamiento de terminal- terminal dentro de la estructura de red de TRDA esta basado en protocolos de internet (IP: Internet protocol). Un grupo de redes puede estar formado por elementos enlazados de un batallón junto con el backbone que enlaza ese grupo con el PC/GU.

45. LA INTERNET TACTICA Y SRMC MEJORADO

a. Las necesidades de comunicaciones de un campo de batalla moderno demanda de la inclusión de interfaces que proporcionen comunicaciones de voz y de datos empaquetados sobre las redes de radio monocanal de combate. Los equipos de radio militares modernos de VHF-FM, hoy en día proveen tres modos de comunicaciones principales: voz segura (codificación y salto de frecuencia), conmutación de paquetes segura y datos seriales seguros.
b. Esta nueva familia de equipos de VHF-FM, cuenta con un amplificador (adaptadas al vehiculo), para dos receptores-trasmisiones y contiene además un controlador de internet que es un ruteador que provee interface para equipos terminales sincrónicos y asincrónicos, equipos terminales de datos u otras del SCBE.
c. Esta familia de equipos no está aún disponible en el ejército del Perú.

46. OTROS COMPONENTES DE LA ARQUITECTURA DE IT

a. El vehículo del G-6/S-6

Está localizado en el PC principal de GU (PC Táctico), conteniendo en su cabina un SISCONI para el planeamiento y control de la IT lo que le permite supervisar su efectividad y apoyar el flujo de info del cmdo entre la IT y el SCBE.

b. Servicio de difusión global (SDG)

En la secc. III del cap. 7 del ME 11-70 se introduce el concepto del SDG, que a nivel GU consiste de puntos de inserción tácticos y de teatro de opns (PIT/TO) y los receptores adecuados. Estos PIT/TO normalmente estarán ubicados en un centro nodal (CN) para permitir a los Cmdtes la teledifusión de grandes volúmenes de info crítica táctica sobre toda la Z/O. Los receptores se ubicarán en todos los PPCC.

c. ETMU mejorado

Este sistema es mejorado porque emplea el modo de transferencia asincronica (ATM) para la conmutación de los sistemas de comunicaciones y el control de los CN's. Todos las demás características son básicamente las mismas a las explicadas en la sección II de este capítulo 2.

d. GPS (Global Position System)

Los receptores GPS son descritos ampliamente en su manual especial y la constelación satelital que los gobierna esta descrita en el ME 11-70. Los receptores están distribuidos en casi todas las unidades de combate y de apoyo de combate; siendo componentes importantes de los plataformas de C^2 y de IT dentro del COTEO y PPCC de los diferentes escalones, para datos de posicionamiento/navegación. Estos datos ingresan al sistema de cmdo de combate de la división y escalones menores, para proveer a la sub arquitectura de conciencia situacional de la IT el apoyo automático de reporte de posición, navegación con punto de vía y otros reportes.

e. Plataformas de C^2

(1) La doctrina de C^2 sobre el movimiento expuesta inicialmente en el ME 11-70 (empleo de comunicaciones satelitales), se materializa en tierra con el desarrollo e implementación de plataformas de C^2. Estas plataformas, no son más que cabinas adecuadamente implementadas con equipos de radio y terminales de computadores y configuradas o reconfiguradas cuando sea necesario, para apoyar a las necesidades de info del cmdte y su intención en la conducción de las opns.

(2) La configuración y reconfiguración de la IT sobre las plataformas se hacen de acuerdo al concepto de opn del cmte , para lo cual cuentan con su software que le permite emitir automáticamente O/O a las unidades subordinados, así como ordenes preparatorias o fragmentarias; manejar datos sobre los factores METT-T y otras funciones de acuerdo a la capacidad de memoria, su velocidad de procesamiento, etc.

(3) El Cmdte, el EM (en particular el G-6/S-6) determinarán las prioridades para la IT y comunicaciones de voz, así como en el POV deberá detallarse el empleo de los mismos. Como un sistema total, la plataforma de C^2 es única, conteniendo diferentes sistemas de hardware y software sobre el mismo vehículo, así como los routers, servidores y particularmente al personal especialista en su opn.

(4) Dos tipos plataformas se han diseñado: vehículo de C^2 y vehículo de cmdo de batalla. Estos vehículos cuentan con estaciones de trabajo (workstation) que manejan los subsistemas de voz radios, intercomunicaciones, recepción de datos, etc; de los sistemas externos vía medios de comunicación móviles terrestres y satelitales.

CAPITULO 3
SEGUNDA DISCIPLINA DEL APOYO DE TELEMÁTICA: ADMINISTRACION DE LA AUTOMATIZACION

SECCION I. INTRODUCCION A LA AUTOMATIZACION

47. CONCEPTO DE AUTOMATIZACION

a. La automatización consiste en la conversión de un proceso o procedimiento manual a operaciones automáticas. Cuando esta automatización está asociada con los medios y facilidades de comunicaciones, puede incluir que la conversión del procesamiento de mensajes a operaciones automáticas se realice en un conmutador, un terminal remoto o una red de área local (LAN).

b. Dentro del sistema del comando de batalla del ejército (SCBE), estas conversiones de procesos a opns automáticas se realizan en los puestos de comando de todos los escalones y en el centro de operaciones táctico del EO, así como en los sistemas operacionales del campo de batalla (SOC´s). Todos ellos emplean hardware y software de computadoras para varios propósitos, sin embargo las unidades o elementos que utilizan para comandar y controlar la maniobra, así como sus operaciones de apoyo de combate se denominan convencionalmente sistemas automatizados del campo de batalla (SAC´s)

48. SISTEMAS AUTOMATIZADOS DEL CAMPO DE BATALLA (SAC´s)

a. Los SAC´s son los medios de los sistemas de información automatizados (SIA´s), empleados por los Cmdtes y sus EEMM para recibir y distribuir información crítica entre todos los escalones. Estos medios de los SIA´s consisten de hardware y software de computadoras que organizan y manejan la info del campo de batalla para su transferencia a los escalones que lo necesitan.

b. Los SIA´s, son cualquier arreglo de hardware, software o firmware de computador; configurado para reunir, crear, comunicar, computar, difundir, procesar, almacenar o controlar datos o información de una forma electrónica. Los SIA´s incluyen computadores independientes, computadores personales, procesadores de palabras, computadores de multipropósito, terminales y redes de computadoras.

c. Los medios del SIA que los SAC´s utilizan consideran a una serie de tecnologías o sistemas de automatización tales como: micrográficos, procesadores de palabras, base de datos logísticos y de personal, análisis financiero-económico, copiadoras computarizadas, procesamiento de datos de propósito general, sistemas de registros electrónicos, impresiones automatizadas, sistemas computarizados de control de telecomunicaciones, entre otras muchas aplicaciones existentes.

d. Los SAC´s deben estar interconectados y comunicados para poder reunir, procesar, difundir y/o transferir con éxito el tráfico de voz, de mensajes, de datos y algo de imagen; tanto desde como hacia el cmdte, su EM y sus escalones superior y subordinado. El G-6, deberá prever y planear los medios que interconecten y comuniquen los SAC´s, para lo cual deberá

visualizar, desarrollar y establecer una arquitectura de comunicaciones tácticas automatizada que se divide en redes de área amplia o WAN´s, tales como los SCAUC, SRMC, sistema de distribución de datos del ejército (SDDE), sistema de comunicaciones de teledifusión y la internet táctica (IT). Estas WAN han sido tratadas en el capítulo anterior y en la Sección III de este Capítulo se amplia información sobre los SAC´s.

49. REDES DE AREA LOCAL PARA EL COT Y PUESTOS DE COMANDO

a. El capítulo 7 del ME 11-30 (Organización y opns de EM de Comunicaciones), se detallan aspectos doctrinarios sobre el control de las opns, organización del cuartel general, su escalonamiento en puestos de comando y el centro de operaciones táctico (COT). En este manual se amplía dichos aspectos en relación a la automatización de sus procesos y organizaciones.

b. El COT y los puestos de Comando sirven como (Hub) de C^2 del EO/GU/Unidad, para ayudar al cmdte en la sincronización de las operaciones. Muchas de las actividades de coordinación de EM, de planeamiento y monitoreo de eventos claves ocurren en estas facilidades o instalaciones. El personal que trabaja en ellas debe asegurarse que todos los recursos están en el lugar y tiempo correcto, funcionando y trabajando eficiente y efectivamente como un equipo en un ambiente rápido e implacable.

c. Cada miembro, individual y colectivamente, debe entender las funciones de un COT y de un PC, para saber como será su contribución; estas funciones básicamente son:
   (1) Recibir, distribuir y analizar info.
   (2) Suministrar recomendaciones al cmdte.
   (3) Integrar y sincronizar recursos.

d. Un COT o un PC funciona principalmente como un centro de procesamiento de información de un alto volumen de tráfico de mensajes, informes y órdenes; sobre las cuales se deberá actuar, dirigir, informar y decidir. Un eficiente sistema de comunicaciones integrará a todos los miembros o componentes del COT o PC tanto interna como externamente; sin embargo se deberá tener presente que será muy fácil que las unidades experimenten una sobrecarga de info al menos que cuenten con sistemas simples y efectivos que les permita recibir y procesar toda la información. Una red de área local (LAN) puede ser la base de esa simplificación y eficiencia.

e. El diseño físico y organización del COT y/o del PC contribuirá a que tan eficientemente son pasados los mensajes desde una sección de EM a otra; así como tan fácilmente las secciones se comunican con otras. No existe un método estandarizado de cómo deberían configurarse estos elementos, para la transferencia e intercambio de información; aunque en el ME 11-30 se establece una organización básica, la experiencia ha demostrado que un PC y/o COT efectivo ha tenido en común los factores siguientes:
   (1) Un alto grado de organización
   (2) Configurada de tal manera que era funcional a la fuerza que apoyaban y no segregaba a ninguna sección del EM.
   (3) Las áreas de planeamiento estaban separadas de las áreas de control y conducción de las operaciones.

(4) Cada COT y/o PC estaba configurado de manera diferente dependiendo de la misión y equipamiento de la Unidad.

Las redes LAN para el COT y/o PC también serán diferentes y variarán dependiendo de los factores METT-T y consideraciones de asuntos civiles.

f. Concepto y descripción general de LAN

(1) Como se ha manifestado anteriormente una LAN es una red de comunicaciones de datos que interconecta terminales de datos digitales y otros periféricos, enlazados sobre una red y distribuidos en un área localizada.

(2) Una LAN consta de un canal de comunicaciones que conecta una serie de terminales de computadora conectadas a un computador central, o más comúnmente, un grupo de computadoras conectados a otro grupo.

(3) Una LAN está conectada por cables o tecnología inalámbrica, usando el estándar 802.3/802.3u, del IEEE (Institute of Electrical and Electronic Engineers) que es de 100 megabytes por segundo (mbps).

(4) Una LAN puede ser configurada en una multitud de configuraciones dependiendo del COEq´ de la GU/Unidad, pudiendo incluir:

(a) Equipos digitales (computadoras, escaneadores, printer u otros periféricos).

(b) Un medio de comunicaciones que conmute datos de un equipo a otro.

(c) Adaptadores de red que provean a los aparatos interface al medio de comunicaciones.

(d) Una topología física extendiendo el medio entre adaptadores.

(e) Un protocolo de acceso llevado a cabo por los adaptadores para asegurar un uso ordenado del medio.

(f) Un formato lógico para transmitir datos sobre el medio.

(g) Una especificación eléctrica para la codificación y trasmisión de datos.

(5) Los recursos de comunicaciones de una LAN son compartidos entre todos los equipos conectados a la red. Los recursos más comunes que comparten las aplicaciones de una LAN son:

(a) Hardware.- Al compartirse este recurso permite que cada computador de un red tenga acceso y use aparatos que son demasiado costosos para asignarlo a cada usuario.

(b) Software.- Significa compartir frecuentemente la capacidad de almacenamiento del disco duro de un servidor para multiplicar la cantidad de usuarios que puede accesar al software de cada computador.

(c) Información.- Al compartir este recurso permite que todos usen un computador sobre una LAN para accesar a los datos almacenados en otro computador de la red.

(6) En la Sección IV se amplían más detalles sobre las redes LAN.

SECCION II. ADMINISTRACION DE REDES Y SISTEMAS AUTOMATIZADOS

50. MISION DE LA ADMINISTRACION DE REDES Y SISTEMAS (ARS)

a. La misión de la ARS es coordinar, manejar y optimizar el empleo de redes y sistemas. Esto implica informar sobre su operatividad y proveer apoyo para la administración, operación y mantenimiento de equipos o sistemas asignados de: comunicaciones, sistemas de información automatizados (SIA´s) y procesamiento automático de datos (PAD).
b. La ARS posibilita a los cmdtes de las unidades de comunicaciones y a sus EEMM cumplir mejor sus objetivos en apoyo a las misiones operacionales del ejército en una Z/O, distribuyendo al escaso personal y recursos tecnológicos más rápido, más económica y más eficientemente en apoyo directo (A/D) de la fuerza desplegada.
c. Las herramientas y procedimientos de administración de un red automatizada reducen los costos de administración, operación y mantenimiento; así como las necesidades de entrenamiento; mientras se mejora la habilidad para intercambiar información relevante de administración. Esto requiere aplicar estándares comúnmente aceptados y la cooperación de todos los elementos que proporcionan servicios de información.

51. OBJETIVO DE LA ARS

El objetivo de la ARS es proporcionar el mejor apoyo de Telemática a los usuarios, mediante:

a. El conocimiento de las necesidades de los usuarios.
b. El conocimiento de cual arquitectura de red y sistemas (configuración de hardware y software) se requiere para satisfacer las necesidades de los usuarios.
c. La confirmación que exista y/o se implemente la red y sistemas para enfrentar los requerimientos de los usuarios.
d. El empleo de equipos de aplicaciones tecnológicas correctas en apoyo a las necesidades de los usuarios.

52. PRINCIPIOS DE LA ARS

a. Los principios que gobiernan el desarrollo o implementación de las ARS dentro del ejército son:
   (1) Compartir información.
   (2) Compartir la visión de información del espacio de batalla.
   (3) Línea de base estándar.
   (4) Empleo de tecnologías y estándares comerciales.
b. Compartir información
   (1) Ninguna organización por sí sola tendrá la capacidad para tener un completo control sobre todos los componentes que proveen servicios de información a un usuario funcional, por lo que será necesario no sólo compartir información sino también SINFOR y situación del servicio entre las varias organizaciones que proveen y usan los SINFOR y servicios.
   (2) La información a compartir por las múltiples organizaciones sobre los recursos, aseguran que los servicios de administración terminal a terminal se cumplan y colaboren entre ellos en la solución de

problemas y provisión de servicios; permitiéndoles leer (monitorear) información mientras limitan la posibilidad de escribir (controlar) info en su propia organización.

c. Compartir la visión de info del espacio de batalla
   (1) Con el incremento de los servicios de distribución de info, será crítico para los usuarios y proveedores de servicios y SINFOR, apreciar la situación de los principales componentes de servicios de info que están siendo usados.
   (2) Las varias redes y centros de sistemas de opns proveen a los líderes del ejército en todos los escalones con una visión en la situación de aquellos servicios de info, para lo cual se necesitará que la info sea compartida libremente y que esté disponible en todas las instalaciones o centros.
   (3) El compartir info no debería causar la duplicación de datos o implicar compartir las responsabilidades de control más allá de lo necesario para cumplir la misión operacional.

d. Línea de base estándar
   (1) El CCFFAA deberá emitir y/o aprobar las capacidades y las normas de estandarización para todas las fuerzas armadas sobre la ARS tácticos. Las capacidades migrarán a una línea de base común de equipo y software para la ARS.
   (2) Algunas de las condiciones y/o normas para la línea de base común podrían ser:
      (a) Aprobación de capacidades de prototipos no estándar para campaña como un agregado a la línea de base de campaña estándar.
      (b) Conceder que una capacidad no estándar que es única para una ubicación o lugar particular sea considerada como anexo a la misma pero no como parte de la configuración estándar.

e. Empleo de tecnologías y estándares comerciales.
   (1) Esto será importante para la interoperatividad de los sistemas de ARS, en particular para accesar, recuperar, distribuir y almacenar info sobre el estatus de la red y sistemas.
   (2) Los principales estándares abiertos que podrían emplearse son:
      (a) Versión simple de protocolo de administración de red.
      (b) Protocolo común de interface de administarción.
      (c) Administración de red telefónica.
      (d) Protocolo de control de trasmisión/protocolo de internet (TCP/IP).
      (e) Protocolo de transporte de hipertexto.
      (f) Protocolo de administración de monitoreo de red remota.

SECCION III. SISTEMAS AUTOMATIZADOS DEL CAMPO DE BATALLA (SAC´s)

53. CONCEPTOS DE SOC´s

a. Como se ha manifestado, el sistema de comando de batalla del ejército (SCBE) comprende al sistema de comando y control táctico del ejército (SC^2TE), cuya intención es integrar las diversas funciones de comunicaciones y automatización de los sistemas operacionales del campo

de batalla (SOC´s), en una sola infraestrutura coherente y precisa dentro del escalón EO.

b. Los SOC´s son una lista de actividades tácticas críticas que proveen los medios de revisión, de preparación o de ejecución de operaciones en sub-conjuntos abstractos pero interrelacionados. Lo crítico de la revisión será la sincronización y coordinación de actividades no sólo dentro de un SOC, sino entre varios SOC´s, ya que estas actividades no direccionan tiempo, ritmo, reconocimiento, operaciones de información y tácticas.

c. La integración de los SOC´s permitirá ayudar a la administración de la información en el área de C^2 sobre el campo de batalla, permitiendo a los medios de comunicaciones automatizados organizar, almacenar, procesar, integrar y trasmitir la información solicitada y/o producida por las actividades de los cmdtes y sus EEMM conforme ellos comandan y controlan sus fuerzas.

d. Los sistemas automatizados que apoyarán a cada SOC se denominan convencionalmente sistemas automatizados del campo de batalla (SAC´s). Estos SAC´s no son sistemas independientes, sino que necesitarán compartir info a través del campo de batalla, así como conectarse horizontalmente (entre todos los SOC´s) y verticalmente (entre SOC´s de diferentes escalones).

e. Al escalón GU, el sistema de comando de combate de división y menores (SCCDM), también integra a los SOC´s para compartir datos e información de entendimiento situacional y de C^2 que permita a los cmdtes contar con bases de datos que satisfagan sus necesidades de info y le provean un cuadro común relevante orientado a las operaciones de combate.

54. PRINCIPALES SAC´s

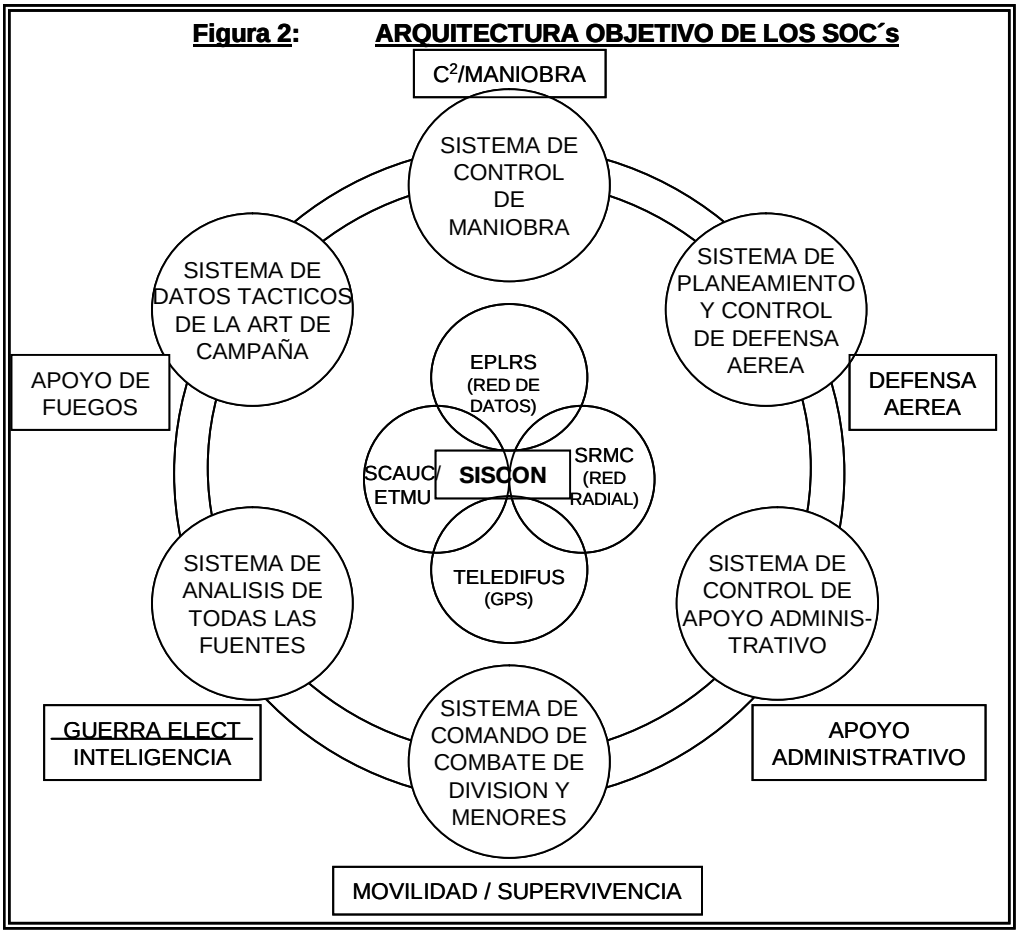
a. Los cmdtes de los equipos de armas combinadas y sus EEMM integran y sincronizan sus SOC´s para ejercer el C^2 de sus fuerzas, mediante la administración, manipulación y evaluación de la info procedentes de ellos y el desarrollo de planes/órdenes tácticas basada en esa info. Los sistemas automatizados del campo de batalla (SAC´s) proporcionan el apoyo de la automatización a los SOC´s en el planeamiento, dirección, coordinación y control de los equipos de armas combinadas; con softwares apropiados que permitan el mantenimiento del estatus de la fuerza, monitoreo de la situación actual, planeamiento de las misiones y control de la transferencia de la info. Los principales SOC´s son: maniobra, apoyo de fuegos, defensa aérea, comando y control, guerra electrónica, inteligencia, apoyo administrativo, movilidad y supervivencia.

b. Los SAC´s principales son los siguientes:
   (1) Sistema de control de maniobra, que apoya a los SOC´s de maniobra y de C^2.
   (2) Sistema de datos tácticos para la artillería de campaña, que apoya al SOC de apoyo de fuegos.
   (3) Sistema de planeamiento y control de defensa aérea que apoya al SOC de defensa aérea.
   (4) Sistema de análisis de todas las fuentes, que apoya a los SOC´s de GE y de inteligencia.
   (5) Sistema de control de apoyo administrativo, que apoya al SOC de apoyo administrativo.

(6) Sistema de comando de combate de división y menores, que apoya al SOC de movilidad y supervivencia.

Estos SAC´s y los SOC´s que apoyan están ilustrados en la figura 2, donde muestra la integración de los sistemas de comunicaciones con los sistemas de información de un campo de batalla moderno para una arquitectura objetivo.

Figura 2: ARQUITECTURA OBJETIVO DE LOS SOC´s



55. SISTEMA DE CONTROL DE MANIOBRA (SCM)

a. La maniobra consiste de equipos de armas combinadas que luchan o se defienden contra una fuerza enemiga. El sistema de comando y control (ver párrafo 05) entrega info esencial al cmdte y a su EM, que satisfagan sus necesidades de C^2.

b. El SCM es el principal SINFOR de maniobra diseñado para proveer ayuda automatizada al cmdte y a su EM para reunir, coordinar y actuar sobre la información del campo de batalla en tiempo casi real; y en la ejecución del concepto de operación del cmdte. Este sistema proporciona un cuadro común relevante y conciencia situacional a los cmdtes, proveyéndoles con ayudas de decisión y capacidades de calcos automatizados sobre las operaciones en curso y futuras, que acorten su ciclo de toma de decisiones en relación al del eno. El SCM transfiere info táctica rápida y exactamente, así como difunde las órdenes del cmdte casi inmediatamente.

c. El SCM proporciona aplicaciones funcionales comunes necesarios para accesar y manipular la base de datos común del SCBE. Esta base de datos mantiene y proyecta info crítica y actual sobre las fuerzas amigas y enemigas obtenida desde los SOC´s, en formatos gráficos o de texto que

los cmdtes y EEMM emplean para identificar posibles formas de acción. Los cmdtes también pueden tomar decisiones de apoyo que concuerden con las decisiones y capacidades de otros cmdtes. El SCM se despliega desde el escalón EO hasta el escalón Batallón de maniobra.

d. Los SCAUC, SRMC y SDDE apoyarán a este sistema, mediante la interconexión de las LAN´s vía internet táctica u otros medios de comunicaciones automatizados.

56. SISTEMA DE DATOS TACTICOS PARA LA ARTILLERIA DE CAMPAÑA (SDTAC)

a. El apoyo de fuegos consiste de fuegos directos o indirectos entregados por los sistemas de la artillería de campaña, los morteros y los fuegos navales y aéreos; contra objetivos terrestres para apoyar al concepto de fuegos del cmdte de una fuerza. La artillería de campaña provee los recursos y pericia necesaria para efectivizar la coordinación del apoyo de fuegos y asesorar su integración con otros recursos de combate.

b. La artillería de campaña cumple su misión proporcionando personal y equipo de apoyo de fuegos en cada escalón de maniobra, estableciendo un centro de coordinación de fuegos colocalizado con el COT y/o PC cuyo director será el cmdte de artillería más antiguo con mando de tropas desempeñándose como coordinador de apoyo de fuegos (CAF).

c. El SDTAC proporciona apoyo a la decisión automatizada para el apoyo de fuegos, que posibilite al cmdte de maniobra influir la batalla. Esta decisión automatizada se materializa a través de un sistema de procesamiento centralizado localizado en el PC de la unidad de artillería, enlazado con sus observadores avanzados, centrales de tiro, centros de coordinación y demás elementos de apoyo de fuegos; mediante radios digitales conectados a equipos de mensajes digitales (Ver párrafo 93 del ME 11-121, doctrina general de GE, Ed 1998) y equipos de entrada de mensajes formateados.

d. El sistema debe contar con hardware y software que provea una adecuada interacción de la mixtura de plataformas de fuego y municiones para enfrentar a los objetivos enemigos de acuerdo al concepto y prioridades del cmdte; al mismo tiempo que facilite al CAF su habilidad para controlar y distribuir sus recursos, mayor movilidad táctica, planear y completar sus misiones en menor tiempo con el mejor sistema de ataque disponible.

e. El SDTAC es un sistema de C^2 de apoyo de fuegos totalmente integrado, que se emplea para planear, coordinar, controlar y ejecutar el apoyo estrecho de fuegos, contrafuego, interdicción y fuegos antiaéreos. Este sistema también debe enfrentar las necesidades de la artillería de campaña para administrar los recursos críticos, reunir y transferir info e inteligencia, controlar los abastos, el manto y otras funciones logísticas de la artillería.

57. SISTEMA DE CONTROL Y PLANEAMIENTO DE DEFENSA AEREA (SCPDA)

a. La defensa aérea consiste en anular o reducir la efectividad de los ataques o de la vigilancia proveniente de aeronaves o misiles enemigos. Un único sistema de armas de defensa aérea no podrá proteger adecuadamente a las fuerzas terrestres o a los lugares críticos, de ahí que normalmente un apropiado sistema de defensa aérea considera una mixtura de sistemas de

armas, interconectados por medios apropiados de comunicaciones para proveer una defensa en profundidad.

b. La defensa aérea ejecuta sus misiones en dos formas: defensa aérea de corto alcance o defensa aérea inmediata y defensa aérea de mediana y alta altitud, dependiendo del escalón en que se ejecute y de la disponibilidad de recursos y unidades asignadas a un TO.

c. Todo este SCPDA, demandará un sistema de C^2 altamente automatizado e intensivo en comunicaciones digitales capaces de soportar la trasmisión de datos, desde las plataformas de fuego de cohetes hasta los más altos niveles de control de defensa aérea. Este sistema debería proporcionar un dedicado y alto volumen de intercambio de voz y datos sobre todo el espacio de batalla en tiempo casi real.

d. El SCPDA ayudará a los administradores de la batalla en el planeamiento, coordinación, sincronización, dirección y control del contra-combate aéreo; asesorándolos en el desarrollo y difusión oportuna sobre datos del objetivo aéreo a todos los componentes de la defensa aérea. Será de particular importancia que los sistemas de radares estén intercomunicados con medios de comunicaciones seguros y flexibles, que provean un seguimiento de identificación de la amenaza, y una alerta temprana automática a los sistemas de defensa aérea.

58. SISTEMA DE ANALISIS DE TODAS LAS FUENTES (SATF)

a. El SATF es un sistema que integra funcionalmente a la inteligencia y a la guerra electrónica, para administrar sensores electromagnéticos y otros recursos que reúnen, procesan y fusionan datos para inteligencia. Este sistema deberá ser capaz de almacenar, manipular y proyectar estos datos y difundirlos rápidamente a todos los cmdtes para proporcionarles un cuadro común relevante de la actividad enemiga para que sea empleado como base de datos por todos los SOC´s.

b. Las cuatro tareas de la misión de las operaciones de guerra electrónica e inteligencia (OGEI) tratadas con detalle en el ME 11-105 (Empleo táctico de GE) en su capítulo 3; son automatizadas bajo este SATF; desde los sensores remotos, los equipos MAGE, radares de vigilancia terrestres y/o perturbadores que operan las unidades de comunicaciones y/o de GE hasta los sistemas de control (SISCON) que administran la búsqueda, reunión y procesamiento. El objeto de esta automatización, como siempre, será la necesidad de la transferencia y explotación de la info e inteligencia en tiempo real.

c. El SATF apoyará al proceso de toma de decisión del cmdte, facilitándoselo y permitiéndole generar oportunidades para alcanzar y retener la iniciativa, proporcionándole info e inteligencia oportuna y precisa que la posibilite maniobrar dentro del ciclo de decisión enemigo, así como mejore significativamente la interoperatividad y apoyo de todos los SOC´s.

59. SISTEMA DE CONTROL DE APOYO ADMINISTRATIVO (SCAA)

a. Este sistema apoya principalmente a las actividades logísticas de mantenimiento, abastecimiento, transporte y servicios médicos; aunque también puede incluir el apoyo a los servicios de personal y de policía militar. La arquitectura objetivo del SCAA es proporcionar sistemas automatizados de hardware y software de computadoras que provean info logística y de personal, que ayuden al cmdte y a su EM a obtener y difundir

info esencial de apoyo administrativo que se requiera para planear y ejecutar la batalla.

b. Aunque el volumen de intercambio de datos entre elementos de apoyo administrativo será relativamente alto, la velocidad de la transferencia de info que se necesitará será baja; de ahí que los sistemas de comunicaciones pueden apoyarlos sin mayores inconvenientes en cualquier parte del campo de batalla tanto para voz como para datos y hasta con imágenes.

c. El SCAA servirá como interface entre el sistema de información de estandarización de apoyo logístico del ejército y los otros SOC´s, consolidando los datos provenientes de los diferentes subsistemas del primero de los nombrados para su empleo por las unidades de apoyo administrativo y/o de combate.

60. OTROS SISTEMAS AUTOMATIZADOS

a. Un sistema importante dentro de un ejército lo constituirá el sistema de info de estandarización de apoyo logístico (SIEAL) que permitirá proveer con datos esenciales para el abastecimiento, reabastecimiento, pedido y reparación de equipos, componentes y/o repuestos.

b. Deberán desarrollarse paquetes de software para cada actividad o función estableciéndose interfaces con otros sistemas automatizados de apoyo administrativo, para que los usuarios puedan maximizar la cantidad de info disponible con la mínima cantidad de datos de entrada; empleándose hardware de uso comercial y sistemas operativos de tecnología multimedia windows.

c. Algunos de los subsistemas del SIEAL podrían ser:
   (1) Sistema de transporte de personal y abasto/equipos
   (2) Sistema de administración de municiones de todo calibre
   (3) Sistema de mantenimiento
   (4) Sistema de abastecimiento de todas las clases
   (5) Sistema de control de stock y cargo de las unidades
   (6) Sistema de listas de cargas prescritas

d. Otro sistema importante lo constituirá la administración del personal del activo y la reserva tanto de personal militar como civil, que demandará el desarrollo de un software y hardware de nivel nacional para facilitar su explotación e integración con sistemas de remuneraciones, pensiones, etc.

e. Finalmente otro sistema que deberá automatizarse de manera independiente lo constituye el apoyo médico, mediante la telemedicina y todas las acciones relacionadas a ella (Ver ME 11-70 sobre la telemedicina de combate).

61. SISTEMAS DE COMUNICACIONES QUE TRANSPORTAN DATOS

a. Los datos se mueven fuera de una red LAN accesando a un sistema de transporte de datos a través de un gateway, que como se ha dicho es una combinación de hardware y software que permite a los usuarios de red accesar a los recursos de otra diferente red.

b. Los sistemas de comunicaciones que pueden emplearse para transportar datos son los siguientes:
   (1) Sistema de comunicaciones de área de usuario común con equipos terminales móviles de usuario (SCAUC/ETMU) y paquete de redes tácticos (PRT).

(2) Sistema de redes de radio monocanal de combate(SRMC)
(3) Sistema de distribución de datos del ejército con sistemas de reporte de posición/localización (SDDE/EPLRS)
(4) Sistema de teledifusión.
(5) Sistemas satelitales.
(6) Sistemas de Comunicaciones permanentes del ejército.
(7) Sistema de correo electrónico del ejército.

SECCION IV. REDES DE AREA LOCAL (LAN) TACTICAS

62. ELEMENTOS DE LAN´s

a. El enlace de SAC´s en un área geográfica local crea una LAN, por la cual viajan los datos que se obtienen y se comparten información. La configuración de la LAN y los protocolos usados dependerán de la misión de la unidad y de la intención del cmdte.
b. Para que una LAN funcione con efectividad, debe ser bien planeada. El hardware, software y los periféricos usados deben interoperar entre ellos. Cada computador central de un SAC tendrá un software único para la función que apoyan, pero de una manera general deben ser capaces de proveer correo electrónico (E-mail), facsímil, intercambio electrónico de datos (EDI: electronic data exchange), almacenar datos de GPS, acceso a internet táctica y videoteleconferencia.
c. Toda configuración de LAN´s deberá contar con los elementos siguientes:
   (1) Tarjeta de interface de red.
   (2) Medio de trasmisión.
   (3) Protocolos de comunicación
   (4) Equipos de conectividad
   (5) Topología de red.

63. TARJETA DE INTERFACE DE RED (TIR)

a. Una TIR es una tarjeta de circuito que se acomoda en una ranura (slot) de expansión de un computador u otro aparato. Muchas tarjetas requieren un cable de conexión y tener conectores sobre la tarjeta para diferentes tipos de cables. Adicionalmente una TIR tiene circuitos que coordinan la trasmisión y recepción de datos y verifica errores de datos trasmitidos.
b. Las TIR´s que son construidas como hardware no se configuran. Para las computadoras laptop, la TIR es la tarjeta interactiva asociada a la memoria del computador personal o más comúnmente conocida como PCMCIA: Personal computer memory card interactive association y puede necesitar o no pequeña configuración.
c. El proceso de configuración de muchas TIR´s diferirán en base a sí ellas están instaladas en un computador – servidor o una workstation. Se necesitarán diferentes “drivers” para sistemas operativos diferentes. Una TIR de una manera general cumple las funciones siguientes:
   (1) Proporcionar alimentación al transceptor
   (2) Interfacea y decodifica memorias receptoras
   (3) Construir memorias para enviarlas fuera de la red
   (4) Interfacear con PC´s y unidades de procesamiento central de PC´s
   (5) Realizar la conversión paralelo a serie

64. MEDIO DE TRASMISION PARA LAN´s

a. Una LAN de un COT/PC puede usar cable coaxial, cable de pares entrecruzados, fibra óptica, alambre, frecuencia de radio, infrarojo o rayos láser. Las Telemática viajarán sobre estos medios de un aparato a otro.

b. Cable Coaxial

(1) Son líneas de comunicaciones de alta calidad y fuertemente aisladas, para reducir su susceptibilidad a la interferencia eléctrica y trasmitir datos de alta velocidad a grandes distancias.

(2) Existen varios tipos de cable coaxial, el más comúnmente empleado en las redes de computadoras es el thinnet o 10Base2 de 0.25 pulgadas de diámetro con conectores BNC (Bayonet Neill Concelman) como terminales y conectores–T para conexiones intermedias. La longitud máxima del cable es de 185 mts y se pueden conectar hasta 30 estaciones separadas cada 50 cm, aunque con repetidores puede aumentarse su rendimiento y capacidad.

(3) Otros tipos de cables coaxiales son:

(a) Thicknet 10 Base 5 de 0.5 pulgadas de diámetro para una longitud de 500 mts para conectar hasta 100 aparatos.

(b) 100 Base–TX a base de cables de cobre para una aparato para una longitud máxima de 200 mts con conectores RJ-45.

c. Cable de pares entrecruzados

(1) Consisten de alambre de cobre aislados con plásticos, entrecruzados juntos por parejas para reducir su interferencia eléctrica. Hay dos tipos conocidos: el STP (Shielded Twisted Pair) que tiene una lámina envolviendo cada alambre y el UTP (Unshielded twisted pair) que no la tiene y es más barato en costo.

(2) El 10 Base T es un cable UTP que popularmente se emplea para conectar workstations a hubs y de hubs a hubs formando una especia de malla-estrella.

d. Cable de fibra óptica

(1) Emplean hilos muy delgados de vidrio o plástico para trasmitir datos como pulsos de luz. Su mayor ventaja sobre los otros dos, es su mayor capacidad para trasmitir datos y comunicaciones de voz simultáneamente, además que su menor peso y tamaño le da mayor rendimiento y alcance; sin embargo su instalación y reparación es complicada.

(2) Existen varios tipos de cable de fibra óptica que pueden cubrir distancias de hasta 2 kms desde 10 mbps hasta 100 mbps tales como 10 Base FL y 100 Base FX.

e. Inalámbricos

Son todos aquellos que usan la radiofrecuencia para trasmitir datos, que dependiendo de la tecnología pueden ir desde 1200 bps hasta el orden de Gigabits.

65. PROTOCOLOS DE COMUNICACIÓN PARA LAN´s

a. Un protocolo es un conjunto de reglas y procedimientos para intercambiar info entre computadoras. Los protocolos se definen de acuerdo a: como se han establecido los enlaces de comunicaciones, como se trasmite la info y como se detectan y corrigen los errores.

b. Los protocolos más comúnmente empleados son:

(1) Ethernet
   (a) Está basado en una topología bus pero puede instalarse como patrón estrella usando un hub alámbrico. Puede trasmitir datos en red desde 10 hasta 100mbps (fast ethernet).
   (b) Un paquete de datos; conteniendo las direcciones de envío y destino se envían a lo largo de la red hasta llegar a su aparato de destino, si ocurriera alguna interrupción una tarjeta adaptadora de red enviará una señal para detener la trasmisión y calculará cuando retrasmitir los datos.
(2) Token ring
   (a) Consiste de una señal de advertencia que circula sobre toda la red LAN para avisar cuando una estación tiene un mensaje para enviar o recibir.
   (b) Las redes de token ring normalmente usan cables UTP.

66. EQUIPOS DE CONECTIVIDAD

a. Los equipos de conectividad más comúnmente conocidos son:
   (1) Ruteadores (routers)
   (2) Conmutadores (switches)
   (3) Puentes (bridges)
   (4) Repetidores (repeaters)
   (5) Concentradores (hubs)

b. Ruteadores (routers)
   Permiten direccionar los cambios conforme, se necesite saltar y/o dividir las opns de una LAN de COT/PC y normalmente se usan cuando algunas redes están conectadas juntas. Un ruteador es un equipo de conectividad de red inteligente que envía (enruta) comunicaciones directamente a la red apropiada. En el caso eventual que falle una red, el ruteador tendrá la suficiente inteligencia para determinar rutas alternas.

c. Conmutadores (switches)
   Conectan segmentos de LAN y un puerto de alta velocidad, para cual tiene un ancho de banda dedicado por puerto. Los conmutadores tienen tablas que asocian direcciones de cada aparato local conectado a un número de puerto, para establecer los enlaces.

d. Puentes (bridges)
   Es una aparato conectado a dos o más LAN´s que usan protocolos idénticos.

e. Repetidores (repeaters)
   Proporcionan la más barata y menos inteligente conexión entre segmentos de una LAN o entre LAN´s localizadas cerca. Los repetidores simplemente toman la señal de entrada y la regeneran sobre otros puertos en el repetidor a su voltaje original.

f. Concentradores (HUB)
   Los concentradores alámbricos permiten a los equipos tales como computadoras, impresoras y almacenadoras conectarse a un servidor, actuando como un punto de conexión central para cables que van desde el servidor a cada aparato sobre una red.

67. TOPOLOGIA DE RED

a. La topología es la manera como el equipamiento es configurado en una LAN. La conexión lógica de los aparatos en la red determinará la topología y el enlace de los datos seguirá la ruta de un aparato al otro.

b. Las topologías más comunes son:

(1) Red Bus

Cuando todos los aparatos o nodos en la red están conectados para formar un enlace simple, permitiendo que los datos se trasmitan en ambas direcciones. Una ventaja de esta topología es que los aparatos pueden agregarse o desagregarse de la red en cualquier punto sin perturbar al resto.

(2) Red Estrella

Cuando tiene un computador central con uno o más terminales o computadores pequeños conectados en forma de estrella. Su mayor desventaja es que la red es dependiente del hardware o software del computador central y si esta falla, la red cae.

(3) Red Anillo

Cuando todos los aparatos en la red están conectados en un loop o anillo. En este caso no se usa un computador host centralizado sino un círculo de computadoras comunicadas con otra. Los datos viajan alrededor de una sola dirección pasando a través de cada computador hasta su destino. Igual como en la anterior topología, si un computador falla, toda la red cae.

68. CONFIGURACION DE LAN´s TACTICAS

a. Las LAN´s tácticas están montadas sobre cabinas especialmente acondicionadas para el C^2 de algún SOC, todas ellas interconectadas con ruteadores formando una LAN externa, manteniendo su protocolo de internet el host que los gobierna. La configuración puede ser en estrella o bus.

b. Cuando es en estrella las LAN´s se conectan a un conmutador central Ethernet. Uno de los vehículos puede contener el acceso a la WAN para conectar al PC/COT a la red o sistema mayor.

c. La configuración final de una LAN táctica dependerá del tipo de unidad, misión y concepto de la opn del cmdte. Los G-6´s/S-6´s en todos los escalones deberán desarrollar una interacción rutinaria con el EM de la Unidad y tomar un rol activo en el proceso de planeamiento, de tal manera de poder iniciar con anticipación el planeamiento, el diseño, la ingeniería, el mantenimiento y la evaluación de la administración de la LAN, particularmente para las redes de protocolo internet.

d. Mayor información sobre las LAN´s y su administración serán desarrolladas en un manual especial.

CAPITULO 4
TERCERA DISCIPLINA DEL APOYO DE TELEMÁTICA: INFORMACION VISUAL

SECCIÓN I. INTRODUCCION A LAS OPERACIONES DE INFORMACION VISUAL

69. CONCEPTO DE INFORMACION VISUAL (IV)

La IV es el uso de uno o más medios visuales con o sin sonido para comunicar información, esto incluye fotograma fotográfico convencional, vídeo digital lento (de imagen congelada), vídeo full motion (grabación o televisión), película en movimiento convencional, ilustraciones generadas manualmente o por computadoras, presentación visual en mono o multimedia y grabaciones de audio.

70. INFORMACIÓN VISUAL TACTICA (IVT)

a. Es la documentación de las operaciones militares a través del procesamiento, trasmisión, reproducción y distribución de imágenes visuales, productos gráficos, la operación de videoteleconferencia (VTC) y servicios de presentación en multimedia dentro de un ambiente táctico u operacional.

b. La IVT incluye a la cámara de combate y servicios de información visual funcional:

(1) Cámara de combate (CAMCOM)

(a) La CAMCOM como concepto doctrinario tiene como misión documentar las actividades de las unidades de combate y de apoyo de combate, para emplear esa documentación para el proceso de toma de decisión operacional y como registros históricos gráficos.

(b) La CAMCOM como equipo son cámaras fotográficas o de vídeo digital operados por personal especializado de comunicaciones para obtener imágenes visuales, instantáneas y/o secuenciales y trasmitirlas por cualquier medio hacia los usuarios que lo solicitan o lo explotarán .

(c) Los elementos/sub-unidades de CAMCOM documentan gráfica o visualmente todas las operaciones o eventos sin considerar la clasificación o sensibilidad de la info. La decisión sobre su clasificación, sensibilidad o revelación/publicación o conocimiento general será hecha posteriormente a través de las coordinaciones de EM.

(d) Los requerimientos de imágenes de CAMCOM incluyen:

1. Grabar o documentar acciones claves antes, durante y después de las fases o etapas de las opns.
2. Evaluación de la efectividad de las preparaciones de la fuerza, objetivos y opns de apoyo e identificación de problemas.
3. Evaluación de la efectividad de los sistemas de armas, actividades relacionadas a inteligencia, apoyo médico,

propósitos de relaciones públicas y contrarestar propaganda enemiga.

4. Documentación histórica gráfica.

(2) Apoyo de información visual funcional

(a) Este apoyo considera a servicios que son establecidos, instalados, operados y su manto operacional orgánico, es realizado por los propios usuarios con los equipos asignados a su organización y no incluye CAMCOM.

(b) El propósito principal de estos servicios es proveer apoyo único y singular a las necesidades de info y toma de decisión de un cmdte específico. Ejemplos de apoyo de IV funcional son las actividades orgánicas de la inteligencia militar, opns/sicolog, relaciones públicas, unidades médicas y fuerzas especiales.

c. Los recursos de IVT estarán normalmente en los escalones EO y superiores. A nivel DE y menores los G-6´s/S-6´s deberán solicitar apoyo de IV al G-6 del EO cuando se requiera, quien asesorará a su comando y comandos subordinados sobre la dirección de los recursos de IV, mediante el establecimiento de políticas y directivas que apoyen la misión asignada. Esto incluye:

(1) El establecimiento de políticas y procedimientos de IV.

(2) Mantener informado al cmdte sobre las capacidades/limitaciones de los elementos/unidades de CAMCOM y los procedimientos para solicitar el apoyo de éstos.

(3) Integración de la IV para apoyar a los SOC´s a su nivel de comando.

71. MSION DE LA IVT

a. La misión de la IVT es proporcionar a los cmdtes y EEMM con productos y servicios visuales en apoyo de todas las áreas funcionales incluyendo operaciones, comando y control, logística, inteligencia militar, ingeniería, relaciones públicas, personal, unidades médicas, policía militar, fuerzas especiales, operaciones sicológicas, asuntos civiles e historia militar.

b. Las funciones que se excluyen de la misión de la IVT son:

(1) Reproducción fotomecánica, cartografía, rayos “x” y producción de microfichas y micropelículas.

(2) Info de C^2 proyectada sobre sistemas de armas.

(3) Imágenes reunidas exclusivamente para vigilancia, reconocimiento o inteligencia; así como equipamiento de IV integrado a vehículos de MAGE.

(4) Imágenes que empleen opns criptológicas.

SECCION II. CAPACIDADES DE LA INFORMACION EN UN AMBIENTE TACTICO

72. INTRODUCCION SOBRE LAS CAPACIDADES DE IV

a. Las unidades o elementos de IV en un ambiente táctico deben tener la capacidad para apoyar las necesidades de IV de cada nivel de comando en su zona de responsabilidad. Las capacidades de IVT son ejecutadas con sistemas y procedimientos de IV compatible con aquellos que el ejército ha estandarizado, empleándose donde sea posible los sistemas de

comunicaciones tácticos y comerciales para proveer la trasmisión de imágenes en tiempo casi real hacia las zonas de combate.

b. Las capacidades de IVT incluyen documentación, procesamiento de productos de IV y la integración de los varios medios gráficos, de vídeo, fotográficos y/o de audio en el proceso de toma de decisión operacional y táctico. Para ello la CAMCOM debe ser móvil, capaz de supervivir y de usar los sistemas de comunicaciones comerciales, tácticos y/o estratégicos para trasmitir imágenes visuales en tiempo real o casi real desde cualquier parte del campo de batalla.

73. CONCEPTO SOBRE DOCUMENTACIÓN DE IV

a. La documentación es la grabación sencilla de cualquier asunto o acción conforme ocurra. Puede ser más adelante integrada o incluida en un medio de producción en movimiento, presentación multimedia o en una serie de imágenes fotogramétricas para un propósito particular.
b. Las unidades/elementos de IV apoyan a las misiones tácticas del ejército con la capacidad de registrar imágenes congeladas o en movimiento, crear imágenes gráficas y grabar información de audio normalmente con el medio de registro de imágenes en movimiento; proporcionando cobertura terrestre y helitransportada a los usuarios o solicitantes que provean transporte.
c. Las tropas de las unidades de CAMCOM usan sistemas de cámaras durables, confiables y livianas; con lentes, accesorios y dispositivos apropiados para permitir la cobertura bajo cualquier situación táctica, incluyendo clima extremo o de poca visibilidad.
d. Las unidades/elemento de IV tienen la capacidad de enviar documentación de actividades significativas a través de los canales de comando y/o técnico; así como deberán mantener un archivo y/o registro de copias de todo el material producido.
e. La documentación puede convertirse a un formato digital para su trasmisión, almacenamiento, recuperación, proyección o procesamiento a un medio convencional (tales como fotos, dispositivos, slides, vídeo-tape o presentación multimedia).

74. RESULTADOS O PRODUCTOS DE LA DOCUMENTACIÓN DE IV

La documentación resultante de las capacidades de CAMCOM incluyen:

a. Operaciones militares en preparación para el “día uno” del combate
b. Posiciones amigas antes, durante y después del combate
c. Posiciones, fortificaciones y obstáculos enemigos antes y después del combate.
d. Documentación sobre el análisis del terreno para apoyar la maniobrabilidad operacional, planeamiento del tránsito/tráfico y ubicación e identificación de barreras.
e. Imágenes aéreas o satelitales de posiciones amigas y enemigas.
f. Imágenes sobre daños de equipos de fuerzas amigas que den a los investigadores y planificadores tácticos, logísticos y de adquisición/desarrollo; info inmediata para desarrollar contramedidas efectivas.
g. Imágenes sobre daños de equipos enemigos para mostrar a los tácticos y logísticos la efectividad de las armas amigas y vulnerabilidades enemigas.
h. Imágenes de abastos, material, equipo, personal y documentos capturados al enmigo; para evaluar el combate, apoyo de combate y apoyo

administrativo enemigo. Estas imágenes pueden ser importantes para las unidades de inteligencia, elementos de opns/sicolog, policía militar y elementos de relaciones públicas; además de servir a historiadores militares y para el archivo histórico-militar.

i. Evidencia para la persecución de crímenes de guerra.
j. Material doctrinario y de combate para instrucción y entrenamiento.

75. FORMAS DE APOYO DE ELEMENTOS/UNIDADES DE IV

Todos los elementos/unidades de IV deberán proporcionar personal especialista, equipo y apoyo de procesamiento que se requiera para cumplir una tarea. Sin embargo las unidades o elementos que soliciten el apoyo de CAMCOM para obtener imágenes deberán proporcionar apoyo en las áreas siguientes:

a. Insumos para el funcionamiento de equipos.
b. Alimentación, transporte y alojamiento al personal especialista
c. Apoyo de EM para coordinación y misionamiento de opns de IV
d. Apoyo de helicóptero y aeronaves de ala fija para imágenes aéreas.
e. Expertos en asuntos específicos para obtención de imágenes que satisfagan sus necesidades.

76. CAPACIDADES DE LOS MEDIOS Y METODOS DE IV

a. MEDIOS PARA IMÁGENES EN MOVIMIENTO
   (1) La tecnología para captar imágenes en movimiento es un medio poderoso de comunicación masiva e individual, cuyos productos o resultados informarán a las tropas y público en general; de estudios en adoctrinamiento, entrenamiento y para propósitos específicos del comando e info pública.
   (2) Estos productos proporcionan a los cmdtes la capacidad para revisar las opns y entrenamiento de sus fuerzas e introducir técnicas nuevas y mejoras operacionales. Las unidades que se muevan a nuevas posiciones pueden ser orientadas con imágenes en movimiento sobre el terreno en que se desplazarán.
   (3) La tecnología de medios para movimiento puede usarse para opns diurnas, nocturnas y/o de visibilidad limitada; proporcionando a los cmdtes las capacidades de apoyo siguientes:
      (a) Documentación de vídeotape de formato pequeño (tales como 8 mm banda alta), para aplicación en combate que requieran luz y sistemas portátiles que produzcan imágenes de aceptable calidad.
      (b) Documentación de videotape de formato de producción (tal como betacam), para aplicaciones como original en vídeo encriptado y transferencia a formato digital de CAMCOM para reproducción posterior y distribución a usuarios, tales como teledifusión o apoyo a RP y Opns/sicolog.
      (c) Producción de informes en vídeo editado en grueso para aplicaciones en apoyo al Cmdte y su EM en niveles btn/GU.
      (d) Producción de vídeo totalmente editado para niveles EO y superiores.
      (e) Interconectividad de comunicaciones.- Para convertir las películas e imágenes electrónicas analógicas a formato digital para su trasmisión sobre sistemas tácticos o estratégicos del ejército; o por sistemas comerciales terrestres o satelitales:

1. Hay que tener presente que la trasmisión de Telemática de vídeo no encriptado requiere un circuito acondicionado para un ancho de banda de 6Mhz y si se encripta demandará un circuito de 6.3 Mhz.
2. El empleo de tecnologías de comprensión de Telemática de vídeo permitirán reducir el ancho de banda requerido a solo 4.5 Mhz.
3. Para la trasmisión en tiempo real de vídeo en movimiento se necesitará que las unidades/elementos tengan capacidad para accesar a sistemas comerciales en bandas Ku o C satelitales.

b. MEDIOS DE VIDEO DIGITAL FOTOGRAMETRICO (VDF)

(1) El vídeo digital fotogramétrico posibilita la trasmisión oportuna de imágenes fotográficas críticas tales como características del terreno, despliegues tácticos, info para inteligencia y opns tácticas directamente desde el campo de batalla proporcionando a los cmdtes con imágenes fotográficas en tiempo casi real para mejorar su toma de decisiones operacionales.

(2) Las cámaras del VDF usan floppy disk de 2.5 pulgadas para capturar electrónicamente imágenes con impresiones a color disponible en segundos en impresoras a color (actualmente las cámaras digitales emplean CD´s de tamaño pequeño con mayor capacidad y resolución):

(a) Estas cámaras digitales tienen aparatos de visión nocturna, pueden trasmitir las imágenes sobre sistemas de comunicaciones digitales militares y comerciales.

(b) El floppy dissk (o CD) puede copiarse, transportarse por mensajero o courier a ubicaciones o usuarios operacionales.

(c) Actualmente se puede usar modem sobre líneas de 4 hilos acondicionados de 300 a 9600 baudios; pero también sobre medios inhalámbricos digitales. A 300 baudios una trasmisión de imagen de VDF demora 14 minutos y a 9600 baudios 3 minutos.

c. DOCUMENTACIÓN FOTOGRAMETRICA BASADA EN PELICULA

(1) Para misiones de IVT que requieran imágenes fotográficas de alta calidad, las unidades/elementos de IV tienen la capacidad de toma de fotografías de tecnologías de películas. El fotógrafo debe de manera expeditiva revelar las películas con una leyenda o título completo para su procesamiento e impresión.

(2) Seria ideal que se contará con laboratorios móviles de campaña para el revelado a color y en blanco y negro, así como impresoras, reproductoras de tomas fotográficas para las copias necesarias que documenten la acción, hecho o actividad para todos los cmdtes y elementos necesarios.

d. DOCUMENTACIÓN DE AUDIO

Las unidades/elementos de IV deben mantener una capacidad para proporcionar documentación de audio en apoyo de misiones tácticas, la cual será proporcionada por micrófonos portátiles, grabadoras de mano de audio o por sistemas de audio integrados con las videograbadoras. Esta grabación y equipos de audio deben usar tecnologías de sonido de alta fidelidad y cassetts magnéticos de tamaño estándar y los ahora populares mini-cassetts, así como CD´s de sonido.

e. GRAFICOS
   (1) El diseño, creación y preparación de gráficos de dos y tres dimensiones (3D) manualmente o con apoyo de computador con programas tipo windows, graficadores, autocad, etc; será una responsabilidad permanente de los especialistas de las unidades/elementos de IV.
   (2) En un ambiente táctico, estas unidades /elementos de IV realizarán algunas tareas críticas para el cmdte, referidas a gráficos:
      (a) Producción de gráficos operacionales precisos para decisión y/o info.
      (b) Mejoramiento de mapas, fotografías aéreas e imágenes satelitales
      (c) Creación de calcos, esquemas y/o diagramas del terreno, posiciones y zona del objetivo.
      (d) Incorporación de la imagen visual en los sistemas de control de maniobra (SCM) para mejorar la exactitud de la representación del campo de batalla.
   (3) Los especialistas de documentación gráfica también prepararán cuadros, diagramas, posters y material visual para trípticos, brochures, cubiertas de publicaciones, etc; para propósitos operacionales e históricos.

77. VIDEO TELECONFERENCIA (VTC)

a. Las capacidades de VTC en apoyo a las misiones tácticas van desde el audio simple orientado al usuario y sistemas de proyección de vídeo en los COT/PC´s hasta sistemas de presentación de multimedia automática en COT y PPCC de EO y superiores.
b. El apoyo de la VTC permitirá la interacción entre los participantes enlazados por sistemas de comunicaciones militares, comerciales o integración de ambos en tiempo real. Las capacidades incluyen comunicaciones de audio y vídeo electrónico de dos vías entre dos o más ubicaciones o lugares; o una interacción total de audio y vídeo de una vía.

78. PRODUCTOS MULTIMEDIA

a. Los elementos de Información Visual deberán mantener la capacidad de combinar las imágenes en película de tomas de instantáneas, imágenes en movimiento y documentación gráfica en productos de IV que satisfagan las necesidades específicas de información para apoyo a los Cmdtes tácticos o estratégicos. Ejemplos de estos productos incluyen los informes en vídeo y en multimedia (CD´s, etc.).
b. Los Informes en vídeo son distribuidos en formato de “VIDEO HOME SYSTEM (VHS)” de ½ pulgada. Un informe de vídeo puede ser una secuencia editada sin compresión de documentación CAMCOM con gráficos simples, con o sin narración, usada como un producto “rápido y original” para las necesidades operativas inmediatas del cmdte táctico. Tales informes de vídeo serán producidos por el elemento de CAMCOM de apoyo. Un informe en vídeo para un requerimiento estratégico o táctico será editado de acuerdo a una narración escrita con documentación CAMCOM, gráficos sofisticados, algunos efectos especiales y narración de audio. Los elementos de IV podrían producir tales informes en apoyo a los cuarteles generales de un TO. Los informes en vídeo tendrán un contenido (mensajes) para uso de corto plazo no mayor de un año. Estos informes no son calificados como “producciones” que requieran una administración de

largo plazo aprobadas por el Cmdo del más alto escalón autorizado para ello.

c. Producto multimedia son hechos típicamente en formato digital. Estos productos pueden incluir medios en movimiento, películas fotográficas, gráficos y narración de audio que es almacenado digitalmente y ensamblada (cargada) en un computador. Ejemplos pueden ser: pantalla de proyección gigante, disco láser, lectora óptica de caracteres, estaciones de trabajo tipo PC, puertos (gateway), imágenes satelitales, cámaras fotográficas digitales, videocamaras digitales, grabadoras de vídeo, impresoras, escaners, copiadoras digitales, facsímil (gpo 4), memorias auxiliares, sistemas de simulación, sistemas de modeling, etc.

79. MANEJO Y DISTRIBUCION DE LOS PRODUCTOS DE IV

a. La explotación y manejo de todos los productos de IV sigue un procedimiento básico de cuatro pasos: procesamiento, trasmisión, reproducción y distribución.

b. Servicios de procesamiento, incluyen entre otras:
   (1) Conversión de los negativos de película convencional, slides y de transparencias a imágenes electrónicas para su trasmisión posterior.
   (2) Trasmisión de imágenes fotográficas sobre equipos de radio de combate VHF-FM, sistemas telefónicos tácticos y sistemas satelitales.
   (3) Hacer impresiones o transparencias a color desde imágenes electrónicas.
   (4) Revisión de imágenes fotográficas y en movimiento para rápidos y refinados reportes de vídeo.
   (5) Duplicación y distribución de reportes de vídeo y de imágenes fotográficas.
   (6) Procesamiento de negativos de películas y películas slide a color con procedimientos químicos convencionales, para mantenerlos como archivo o reserva.
   (7) Mantenimiento y reparación de equipo de IV.

c. Trasmisión
   (1) La trasmisión o movimiento electrónico de productos de IV es por:
      (a) Tranceptores digitales conectados a cámaras de vídeo.
      (b) Sistemas telefónicos tácticos militares
      (c) Sistemas satelitales
      (d) Redes radiales de microondas
      (e) Sistema comerciales (alquilando circuitos)
   (2) El movimiento de productos de IV no electrónicos es por:
      (a) Servicio de mensajero
      (b) Correo oficial
      (c) Courier comercial
      (d) Oficial de enlace
      (e) Otros con la seguridad del caso

d. Distribución, la distribución de imágenes de IV es priorizada como sigue:
   (1) Comandante en escena (operando en el campo de batalla)
   (2) Comandante de la fuerza de tarea conjunta
   (3) Comandante de unidad de apoyo
   (4) Oficial de relación públicas, cuando sea apropiado
   (5) Para el registro histórico

SECCION III. APOYO DE CAMARA DE COMBATE Y DE INFORMACIÓN VISUAL FUNCIONAL

80. APOYO DE CAMARA DE COMBATE (CAMCOM)

a. La CAMCOM proporciona a los cmdtes , quienes no necesariamente estarán en la escena de despliegue, la habilidad para visualizar las operaciones en curso. Las necesidades de CAMCOM no son las necesidades de relaciones públicas (RP) o fuentes para los medios de prensa, aunque eventualmente pueden usarse para esos propósitos.

b. El principal propósito de la CAMCOM es su empleo como una herramienta más para el proceso de toma de decisión operacional; por lo tanto a los elementos/unidades de CAMCOM se les debe permitir obtener tomas fotográficas digitales y/o de vídeo de todos los aspectos de una operación o evento sin importar la clasificación o sensibilidad. Como ya se ha manifestado, las decisiones sobre la clasificación, sensibilidad o develación puede hacerse después a través de los canales de comando, de inteligencia, de operaciones y de coordinación con relaciones públicas.

c. Durante la documentación operacional, será importante mantener el realismo y espontaneidad. El personal de CAMCOM deberá documentar la acción tal como aparece, no debiendo intentar influir una situación o imponer un control sobre la acción. La mayoría de las operaciones de documentación operacional, no se realizan con la intención de ponerlas al conocimiento público; sino que normalmente se realizan para uso interno operacional o informativo.

81. TIPOS DE APOYO DE IV

a. Las cualidades inherentes de la CAMCOM dan lugar a que se emplee de muchas formas para cumplir y documentar las misiones de las unidades de combate y apoyo de combate. Los sistemas de IV serán empleados si sus capacidades pueden convertirlo en el medio más adecuado de enfrentar una necesidad de comunicación operacional.

b. El G-3/S-3 de las unidades de maniobra y de apoyo de combate cuentan con recursos orgánicos de IV, que incluyen a personal técnico especialista en su operación; los cuales pueden emplearse para operar un centro de entrenamiento audiovisual y/o producir ilustraciones gráficas, cartas o diagramas simples y transparencias de mapas. Ellos también pueden ser los operadores del sistema de control de maniobra (SCM) en apoyo al proceso de toma de decisiones, operando independientemente del apoyo proporcionado por los elementos/unidades de IV (CAMCOM).

c. Los elementos/unidades de CAMCOM serán requeridos para el apoyo de mantenimiento especializado y para la obtención, procesamiento, trasmisión, reproducción y distribución de productos de imágenes para apoyar al cumplimiento de la misión, para fines de entrenamiento o de info operacional. Las capacidades orgánicas principales de estos elementos/unidades incluyen:

(1) Computador avanzado para gráficos e impresoras a color de alta resolución.

(2) Proyección de televisión y de vídeo avanzado.

(3) Cámaras fotográficas digitales con medios de transmisión/recepción de imágenes electrónicas.

(4) Librerías/albunes fotográficos digitalizados y archivos de vídeo digital computarizados.

82. APOYO DE IV FUNCIONAL

a. El apoyo de IV funcional son las capacidades (sistemas y equipos) orgánicas a unidades de combate y apoyo de combate. Estas capacidades son operados por las propias unidades y no incluyen CAMCOM, pero si áreas funcionales como gráficos, fotos de película, vídeo de película, proyectores de imágenes fijas o en movimiento y algunas multimedia.

b. El principal propósito de la IV funcional es apoyar a necesitadas particulares o singulares de información y toma de decisión de un cmdte de combate o de apoyo de combate específico. Esto incluye:
   (1) Cobertura terrestre y helitransportada
   (2) Procesamiento de imágenes
   (3) Trasmisión de imágenes
   (4) Reparación de equipos de IV por manto contratado

c. El apoyo de los elementos/unidades de CAMCOM a la capacidad orgánica de IV funcional y de los elementos, actividades u operaciones en un campo de batalla se puede materializar de la manera siguiente:
   (1) Apoyo a las unidades médicas
      (a) Aunque la documentación médica normalmente es realizada por el propio personal médico, las unidades/elementos de CAMCOM aumentan este servicio usando todos los formatos de películas, cinematográficas, vídeo, audio y arte gráfico. Los videos-tape de alta resolución serán los medios preferidos.
      (b) El personal que documentará algún procedimiento médico en alguna sala de opns o quirófano, deberá cumplir con las instrucciones del personal médico sobre la esterilización alrededor del paciente, así como el equipo deberá instalarse lo suficientemente alejado para no estorbar, pero lo suficientemente cerca para grabar el procedimiento.
      (c) El apoyo de microfotografia y microcinematografía será coordinado y demandará el empleo de lentes y adaptadores especiales con sistemas ópticos conectados a las cámaras.
   (2) Apoyo a la inteligencia militar
      (a) Este apoyo estará limitado a la documentación requerida por el G-2 y unidades de inteligencia a escalones EO y GU, para las actividades principales sgtes: documentación de prisioneros de guerra, toma de imágenes de material eno capturado, reproducción de documentos enos, documentación detallada de instalación capturadas al eno, grabación/registro de objetivos especiales, etc. Las unidades/elementos de CAMCOM procesarán, editarán, reproducirán y distribuirán productos de IV capturados a las fzas enas.
      (b) La documentación de inteligencia técnica y de inteligencia estratégica con apoyo de elementos/unidades de CAMCOM deberán ser dirigidos por los especialistas y analistas de inteligencia.
   (3) Apoyo a la Policía militar
      (a) El apoyo de CAMCOM es también en la documentación de todas las actividades del tratamiento a prisioneros de guerra,

procedimientos de protección y control de tránsito y para investigaciones de prebostazgo.

(b) Este apoyo se hace para mostrar como se trata a los prisioneros de guerra (identificación, registro, cuidado, salud, moral, etc); para documentar como se protege la zona de retaguardia (camuflaje, potenciales campos de fuego, preparación de obstáculos, etc).

(4) Apoyo a las opns/sicolog

(a) Los elementos/unidades de CAMCOM refuerzanlas capacidades de los elementos de opns/sicolog en la producción de imágenes con mensajes de opns/sicolog efectivos orientados a la población civil y al enemigo.

(b) Las ilustraciones gráficas, las fotografías de películas y los reportes de videotape proveeran cobertura de apoyo a las opns sicológicas y mejorarán el valor del material impreso y de difusión radial y televisivo con objetivos sicológicos, tales como:

1. La documentación de desertores, soldados enemigos o refugiados siendo tratados bien o proporcionándoles ayuda humanitaria, comida, tratamiento médico, alojamiento adecuado, etc.
2. La documentación mostrando la evidencia de superioridad amiga en vestuario, equipo, armas, municiones, vehículos, etc.
3. La documentación obtenida de fuentes enemigas que los desacrediten.
4. Fotografías aéreas o satelitales que muestren instalaciones, fortificaciones, fábricas y facilidades de comunicaciones enas que están destruidas.

(5) Apoyo a las relaciones públicas (RP)

(a) Aunque las capacidades de IV de las RP son bastantes similares a las de los elementos/unidades de CAMCOM, las misiones y los usuarios finales de sus productos difieren grandemente. Los recursos de RP no se usan en un rol de documentación de combate e igualmente los recursos de CAMCOM no son usados principalmente para propósitos de RP; sin embargo los medios fotográficos y de vídeo de ambos, pueden emplearse para complementar sus misiones uno al otro.

(b) Como se ha manifestado, la misión de la CAMCOM es proveer documentación visual de combate en la toma de decisión operacional y para crear un registro visual de las opns de la unidad sobre el campo de batalla. En cambio la misión de RP sobre el campo de batalla es provocar la multiplicación de la información de comando e información pública:

1. La información de comando es un multiplicador de combate de probada eficacia y es la más importante función de RP sobre el campo de batalla. El cmdte, a través de su oficial u oficina de RP, usa la info de comando para mantener a sus soldados informados donde ellos se colocan, que se espera de ellos y como ayudarán a cumplir la misión (Ver párrafo 26 del ME11-13, Opns de info, Ed 1999).

2. La información pública es la obtención y difusión de info directamente hacia el público nacional e internacional a través de los medios de comunicación civiles.

(c) Las unidades/elementos de CAMCOM pueden aumentar y proveer a las organizaciones de RP, con procesamiento, edición, reproducción, distribución y manto de equipo de IV; pudiendo inclusive accesar a las áreas y a las opns tácticas donde probablemente no ingresan los elementos de RP.

CAPITULO 5
CUARTA DISCIPLINA DE APOYO DE TELEMÁTICA: SERVICIOS DE INFORMACION DEL CAMPO DE BATALLA (SIC)

SECCION I. CONCEPTO OPERACIONAL DE LOS SERVICIOS DE INFO DEL CAMPO DE BATALLA (SIC)

83. ANTECEDENTES DE LOS SIC

a. El G-6/S-6 es responsable por el funcionamiento y administración del sistema de correo oficial del Ejército durante las operaciones que incluye la administración de la correspondencia, mantener registros informativos de informes, formatos, directiva y publicaciones.
   (1) En época de paz, la administración de la correspondencia tradicionalmente ha sido del Oficial del Personal, sin embargo el gran volumen de información que se viene procesando de manera automatizada, crea la necesidad de pasar esta responsabilidad a un nuevo Oficial de EM.
   (2) El establecimiento de un sistema adecuado que permita cumplir con esta tarea, será la clave para proteger toda la información o correspondencia escrita que se produce en el Ejército, del acceso de personal no autorizado.

b. A nivel EO, y superior; el G-6 puede tener la responsabilidad de impresiones y publicaciones durante las operaciones, particularmente en la impresión y reproducción de publicaciones que apoyen a las operaciones de los otros miembros del EM en tiempos y lugares donde no será posible tener medios locales (civiles o militares) a disposición, en el momento.

c. Servicios de Información del Campo de Batalla.- Son aquellos que integran las disciplinas de apoyo de Telemática de administración de registros y de impresiones y publicaciones; incluyendo funciones y recursos empleados para organizar, distribuir, recuperar, disponer y manejar todos los registros sin importar el medio; en un ambiente de combate. En guarnición estos servicios son proporcionados por diferentes dependencias y organizaciones con instalaciones fijas y equipamiento no diseñado para campaña; sin embargo cuando una unidad de maniobra se despliega, el elemento orgánico de apoyo de Telemática de la GU (EO) proporcionará estos servicios de información, con su equipamiento orgánico.
   (1) Administración de registros.- Considera la administración de:
      (a) Formatos.- Son documentos prescritos oficialmente con espacios en blancos preparadas para insertar información.
      (b) Correspondencia.- Se refiere a los medios que pueden producir, reproducir o trasmitir comunicaciones manual o electrónicamente. Pueden ser también medios magnéticos u otras correspondencias o formatos de propósito especial oficialmente autorizados.
      (c) Archivos/registros.- Se refieren a cualquier material creado, salvado o almacenado, que incluye libros, papeles, mapas, fotografías, materiales de máquinas lectoras u otros materiales documentarios sin importar su contenido o su forma física.
      (d) Programas de privacidad individual.- Se refiere al programa de protección de la privacidad de un individuo, asegurando que la

información grabada o archivada referente a él es la estrictamente necesaria, oportuna, precisa, completa y confidencial, de tal manera que no afecte su dignidad, su honor intimidad y que además no se revele a personas no autorizadas.

(e) Documentos clasificados.- Se refiere al control, custodia y almacenamiento temporal de documentos clasificados en espera de su distribución, excepto la documentación estrictamente secreta.

(f) Distribución de correo o mensajes oficiales (incluido el correo electrónico o E–mail). La Distribución y entrega de cartas, mensajes o material impreso normalmente corresponde a los servicios de correos o servicios postales públicos o privados; sin embargo cuando ingresan al ejército, las oficinas postales, mesas de partes se hacen responsables, en guarnición. En campaña y en lugares y circunstancias donde estos servicios no funcionarían el G-6 en coordinación con el G-1, proporciona el servicio de recepción, recopilación, clasificación, reproducción adicional y el apropiado enrutamiento de los mensajes y materiales impresos en una organización específica o entre organizaciones. Todo correo oficial es normalmente dirigido al Cmdte de una unidad militar.

(2) Impresiones y Publicaciones.- Son los procesos de composición de la información y representación de medios, que incluyen fotocomposiciones; empastados, anillados y/o encuadernados para su emisión; y la distribución de los productos terminados:

(a) Impresión.- Es el proceso de composición, trabajo en prensa y encuadernamiento (empastado), colocando imágenes, signos, letras o cualquier información sobre papel en volúmenes superiores a 1000 unidades de un original simple y hasta no más de 10,000 unidades de un documento multipáginas.

(b) Publicación.- Son artículos sobre los cuales la información es impresa o reproducida mecánica o electrónicamente para su distribución. Ellos incluyen directivas, panfletos, posters, trípticos, formatos, manuales, brochures, revistas y periódicos en cualquier imprenta por el ejército.

(c) Reproducción.- Es recrear un documento original por medios mecánicos, que incluyen la impresión, duplicación y copiado por procesadoras de copiado automático, duplicadoras, o máquinas impresoras que usan procesos electrostáticos, térmicos u otros de reproducción

84. RESPONSABILIDADES DE LOS SIC

a. La administración de la info es una responsabilidad de cmdo en todos los escalones. El G-6/S-6 y el cmdte de la unidad de comunicaciones son los elementos que ejecutan el apoyo en campaña, siendo responsables por la administración de los SIC para el cmdte táctico

b. Para cumplir con estas responsabilidades y/o ayudar en ese esfuerzo, en los escalones GU y superiores se deberá crear un puesto o función para un Oficial como miembro del EME denominado Oficial de Apoyo de Servicios de Info (OASI) quién estará bajo el control del G-6. A escalones menores será el S-6 responsable por la administración y ejecución de los SIC , los cuales normalmente serán mínimos.

c. El G-6 proporcionará un marco o procedimiento guía para que los demás miembros del EM operen, obtengan o realicen servicios de info. A su turno el usuario/miembro del EM recibe, pasa y obtiene info dentro del marco del SIC. Aunque el G-6 establecerá el marco y el formato para esos servicios, el proponente/usuario será responsable por su contenido. Por ejemplo, el G-6 será responsable por el control y provisión de orientación sobre la administración de formatos o el desarrollo del sistema de administración de registro uniforme; pero el usuario será responsable por el diseño y contenido de la forma/formato o info contenida dentro del archivo. El OASI establecerá los procedimientos de control de documentos clasificados, pero el usuario será responsable por generar y almacenar el material/documento clasificado.

d. Bajo el control y supervisión del G-6, el OASI coordina y apoya la administración centralizada de las necesidades de SIC al interior de un cuartel general, así como guía y regula los servicios que no estuvieran administrados centralizadamente.

85. ADMINISTRACION DE LOS SIC

a. Los servicios de informaciones del campo de batalla (SIC) pueden ser administrados a través del control directo de la actividad o a través de la emisión o promulgación de políticas.

b. Control directo.- Bajo el control del G-6, un punto de contacto especifico recibe y enruta todos los pedidos concernientes a servicios de info del campo de batalla. La distribución y la reproducción requerirán de la acción o control directo..

(5) Distribución.- El OASI establece un proceso de distribución y será responsable por la distribución interna empleando al servicio de mensajeros. La distribución interna es aquella que se realiza entre elementos del EM del mismo cuartel general incluyendo la correspondencia/correo Oficial. La distribución externa es el movimiento de la correspondencia oficial (incluyendo publicaciones) y la distribución entre puestos de comando. A nivel GU/EO el OASI establecerá un centro de distribución de mensajes/correspondencia.

(6) Necesidades de reproducción.- Estarán centralmente administradas por el OASI, quién recibe los pedidos de impresión del usuario y los enruta hacia la unidad de comunicaciones que cuente con la capacidad de reproducción o hacia la facilidad establecida para tal fin.

c. Administración por políticas.- Cuando el G-6 establece políticas, lineamientos y/o directivas que suplementen las regulaciones permanentes. En este caso los usuarios y miembros del EM serán responsables por la satisfacción de sus propias necesidades de SIC.

SECCION II. IMPRESIONES Y PUBLICACIONES EN CAMPAÑA

86. RESPONSABILIDADES DE IMPRESIONES EN CAMPAÑA

a. No existe capacidad de impresión orgánica en los escalones EO y menores para campaña. Si alguna unidad/GU tuviera un requerimiento grande de impresiones durante sus opns. El OASI validará, priorizará y enviará el pedido a través de los canales establecidos a la organización apropiada, verificando previamente que este en el formato correcto y de acuerdo a las

políticas y directivas emitidas. El OASI no tiene responsabilidad en pedidos de impresiones topográficos, sicológicas o de inteligencia.

b. Aunque no existe capacidad de impresión, las unidades de comunicaciones deberán ser dotadas con aparatos de reproducción tácticos que incluyen computadoras personales tácticas, duplicadores desplegables tácticas, copiadores de documentos tácticas y terminales apropiados. Todos estos aparatos vienen diseñados para operar con energía secundaria y/o energía proporcionada por grupos electrógenos que operan las unidades de comunicaciones.

c. El OASI servirá como un punto de contacto para recepcionar los pedidos de impresión/reproducción a nivel GU/EO.

87. RESPONSABILIDADES DE PUBLICACIONES EN CAMPAÑA

a. El OASI será responsable por la supervisión de las publicaciones en los escalones GU/EO recomendado políticas, procedimientos y convenciones. Cuando una unidad/GU entrara en opns, el C-6/G-6 (EO) asignará a ella un código para solicitud de publicaciones de campaña que le darán una prioridad ante su solicitud en un ambiente táctico. Sin embargo, antes que una unidad/GU se despliegue, deberían asegurarse que cuenten con publicaciones suficientes para cumplir sus misiones en tiempo de guerra por el período de duración estimado.

b. El OASI tendrá las responsabilidades de publicaciones en campaña sgtes:
   (1) Mantener los cargos de las publicaciones de la GU.
   (2) Controlar y preparar un índice de publicaciones del Cuartel general (excepto ordenes de opns)
   (3) Revisar y aprobar las solicitudes de publicaciones y asegurarse que éstas están correctamente formuladas.
   (4) Preparar y presentar pedidos de publicaciones administrativas, de entrenamiento, doctrinarios y técnicos para el EM del cuartel grl.
   (5) Mantener una librería de publicaciones administrativas para el EM

88. RESPONSABILIDADES DE REPRODUCCION

a. El OASI realiza la supervisión y el apoyo de los servicios de reproducción, recomendando políticas, procedimientos y convenciones. Los servicios de reproducción incluyen duplicación, compaginación, encuadernación/anillado y empaquetado.

b. El OASI contará con equipo de reproducción de alto volumen o coordinará con la unidad de comunicaciones para apoyo suplementario/complementario. Además puede contar con fotocopiadoras u otras aparatos similares adaptados para trabajar en un ambiente de combate (acondicionados en vehículos).

c. Los duplicadoras desplegables tácticas serán empleados solamente en campaña y serán asignadas a las unidades de comunicaciones. Estas deben tener la capacidad de 70 copias por minuto o más.

SECCION III. ADMINISTRACION DE REGISTROS

89. RESPONSABILIDAD GENERAL DE LA ADMINISTRACION DE REGISTROS

a. A nivel GU/EO el G-6 será responsable por la supervisión de EM de la correspondencia, archivos y programas de privacidad individual en campaña; que incluye la interpretación y supervisión completa con el

establecimiento de políticas, doctrinas y procedimientos. Sin embargo los otros miembros del EM o usuarios que manejan sus archivos y correspondencias relativos a su campo funcional serán responsables de ellas para sus misiones específicas.

b. Para la correspondencia, el OASI bajo el control del G-6 deberá:
   (1) Realizar la supervisión de EM.
   (2) Recomendar procedimientos locales y convención de autenticación.
   (3) Establecer planes de distribución.
   (4) Recomendar procedimientos locales para la lectura de archivos

90. RESPONSABILIDADES DEL OASI EN LA ADMINISTRACIÓN DE ARCHIVOS

a. Supervisión de EM en la administración de archivos.
b. Recomendar políticas, procedimientos y convenciones.
c. Aprobar lista de archivos y convenciones electrónicas.
d. Verificar la exactitud y proveer orientación sobre la preparación de paquetes que contienen archivos o registros.

91. RESPONSABILIDADES DEL OASI EN EL CONTROL DE DOCUMENTOS CLASIFICADOS

a. En campaña, el OASI será responsable por el control temporal y almacenamiento de documentos clasificados en espera de su distribución, recomendando políticas, procedimientos e inspecciones de documentos clasificados.
b. El OASI no realiza el control de documentos ESTRICTAMENTE SECRETOS.
c. La autoridad de clasificación de los documentos la tiene el cmdte y la distribución es responsabilidad del OASI
d. El control de documentos clasificados como correspondencia o archivo será del usuario, así como de su distribución.

92. RESPONSABILIDADES DEL OASI EN LA DISTRIBUCIÓN DE CORRESPONDENCIA OFICIAL EN CAMPAÑA

a. Supervisión de EM de la distribución.
b. Recomendar políticas, procedimientos y convenciones
c. Mantener los cargos de la distribución incluida la correspondencia oficial.
d. Distribución interna.
e. Coordinar y supervisar servicio de mensajeros/correspondencia en el cuartel general
f. Cumplir con las regulaciones postales en el procesamiento por correo oficial.
g. Recoger y distribuir correspondencia Oficial del elón superior.

CAPITULO 6
QUINTA DISCIPLINA DEL APOYO DE TELEMÁTICA: SEGURIDAD DE LAS INFORMACIONES

SECCION I. ASPECTOS INTRODUCTORIOS SOBRE LA SEGURIDAD, OPERACIONES DE INFORMACION Y GUERRA DE COMANDO Y CONTROL

93. CONSIDERACIONES Y CONCEPTOS GENERALES SOBRE LA SEGURIDAD

a. La doctrina actual de los Ejércitos acepta que el Comandante más hábil en "Visualizar el Campo de Batalla", disfrutará de una ventaja táctica significativa; es decir, el Comandante que dispone de la mejor Inteligencia sobre el campo de batalla y la emplea provechosamente, gozará de una decidida ventaja en el equilibrio de la potencia combativa.

b. Para visualizar el campo de batalla, los esfuerzos de la Inteligencia tradicional se han concentrado sobre el enemigo inmediato a enfrentar. Sin embargo, la experiencia de los últimos conflictos, en donde la tecnología empleada por los Ejércitos, ha influido poderosamente en el equilibrio de las fuerzas, al dar mayor énfasis al empleo de sistemas electrónicos y de comunicaciones; exige un análisis más profundo de otros factores que anteriormente no constituían una amenaza evidente a nuestras fuerzas, antes, durante y después del planeamiento de las operaciones.

c. Los factores o principios que hoy en día han cobrado auge y se han vuelto determinantes, aún sobre el factor numérico o principio de MASA, son los de: SEGURIDAD y SORPRESA. Lograr y conservar estos principios, exigen que nuestros Comandantes puedan impedir que el enemigo utilice su habilidad o capacidad de búsqueda de informaciones o al menos controlar su empleo.

d. **Conceptos Generales sobre la Seguridad**

(1) El concepto de seguridad es inmanente al hombre; la seguridad definida como el conjunto de medidas que cubren cualquier riesgo, genera un estado de confianza y tranquilidad a una persona o grupo, que proviene de la idea de que no hay peligro.

(2) La seguridad es un concepto permanente e integral, ya que es responsabilidad de todos y las medidas se conjugan en todo momento y cualquier descuido en alguna de sus partes puede poner en riesgo al conjunto.

(3) La seguridad descansa en:

(a) La información, que tenemos del enemigo y la que negamos al mismo.

(b) El dispositivo, que nos cubre del riesgo de acciones físicas del enemigo.

(c) Otros elementos, tales como el personal, el material, etc.

(4) La seguridad debe cubrir de todo riesgo a la información, material y al personal, lo que nos dará libertad de acción. Sin embargo se debe tener presente que ninguna medida de seguridad nos garantizará de manera absoluta, que el enemigo no podrá obtener información.

94. CONSIDERACIONES Y CONCEPTOS GENERALES SOBRE LAS OPERACIONES DE INFORMACION

a. Las fuerzas armadas modernas reconocen que la guerra de información es una de las muchas posibilidades del poder nacional de los elementos militares de una nación. La G-I puede apoyar toda una estrategia de gobierno como política de lucha; durante tiempo de paz, crisis, conflicto y post conflicto. La habilidad de un país para influir las percepciones y toma de decisiones de otras países impacta grandemente la efectividad de disuasión, influencia sobre naciones con poder y otras conceptos estratégicos.

b. La G-I está definida como las acciones tomadas para alcanzar superioridad de información mediante la afectación de la información del adversario, de sus procesos basados en información, de sus sistemas de información y de las redes basada en computadoras; defendiendo simultáneamente nuestros mismos procesos, sistemas, redes e información.

c. El Objetivo de la G-I es conseguir una ventaja de información significativa que posibilite a la fuerza en su conjunto, dominar y controlar rápidamente al adversario. La meta estratégica de la G-I es capturar y mantener una ventaja decisiva mediante el ataque a la infraestructura de información nacional (IIN) del adversario a través de su explotación, negación e influencia; al mismo tiempo que se protege los SINFOR amigos. La G-I ofrece a ambos contendores la oportunidad para golpear a distancia con relativa seguridad.

d. La G-I está mas orientada al impacto de la información sobre todo un país durante un conflicto en curso; sin embargo a nivel ejército el concepto de G-I está tomado en un contexto más amplio para orientarlo al impacto de la información sobre las operaciones terrestres en todo el rango de ellas y desde época de paz hasta la guerra total. A esta concepción ampliada de la G-I se le denomina OPERACIONES DE INFORMACIONES (OI), que implementa las políticas de la G-I para un Cmdte del componente terrestre.

e. LA OI están definidas como las operaciones militares continuas dentro del ambiente de información militar (AIM) que posibilita, mejora y protege la habilidad de las fuerzas amigas para reunir, procesar y actuar sobre la información para alcanzar una ventaja a través de todo el rango de la operaciones militares; incluyendo la interacción con el ambiente de información global (AIG) y la explotación o negación de información y posibilidades de decisión de un adversario. Las OI integran todos los aspectos de la información para apoyar y mejorar los elementos del poder de combate (potencia combativa), con el objetivo de dominar el espacio de batalla en el momento y lugar correcto; y con las armas y recursos apropiados. Las unidades conducen OI a través de todo el rango de las operaciones militares, desde las operaciones en guarnición en época de paz, pasando por el despliegue, las operaciones de combate y continuando hasta el redespliegue y completamiento de la misión.

f. Los componentes de las operaciones de información son:
   (1) Operaciones de información propiamente dicha.
   (2) Información relevante e inteligencia (IRI).
   (3) Sistemas de información (SINFOR).

g. Las operaciones de información propiamente dicha, son básicamente las siguientes:

(1) Guerra de comando y control (G-C^2)
(2) Operaciones civiles-militares (o AC: Asuntos Civiles).
(3) Operaciones de relaciones públicas.

95. CONSIDERACIONES Y CONCEPTOS GENERALES SOBRE LA G-C^2

a. La habilidad táctica y un liderazgo efectivo, son los principales elementos de la potencia combativa sobre un moderno campo de batalla aeroterrestre. La tecnología actual ha integrado los factores de tiempo y espacio, que se requieren para unas operaciones de combate efectivas.
b. La alta movilidad de las fuerzas de combate aeroterrestres, así como la velocidad, alcance, precisión, exactitud y letalidad de los sistemas de armas, condicionan las rígidas demandas de los Comandantes y Oficiales del Estado Mayor. Por otro lado, los altamente sofisticados y multidisciplinarios Sistemas de Reconocimiento, Vigilancia y Adquisición de Blancos (S-RVAB), son todos predictivos; y sus computadores reaccionan más rápidas y precisas que el ser humano.
c. Las posibilidades mencionadas en el párrafo anterior cuando están integradas con los factores de tiempo y espacio, contribuyen a la victoria o a la derrota; colocando cada área del campo de batalla en virtualmente INSEGURA.
d. Las instalaciones y sistemas de C^2 son objetivos de Alta Prioridad (OAP) tanto para nuestras fuerzas como para el enemigo, ya que ambos emplearán un vasto "arreglo" de recursos y S-RVAB para identificar y localizar rápidamente estas instalaciones y sistemas, debido a que constituyen el punto neurálgico del proceso de toma de decisiones, al ubicarse en ellos los Puestos de Comando, lugares donde se planea, conduce y sostiene el combate, es decir, se comunica información de combate e inteligencia, se coordinan los apoyos y se proporciona la dirección/conducción de la fuerza como un todo.
e. Los Comandantes enemigos conducirán operaciones intensas de RVAB así como realizarán un planeamiento detallado antes de empezar una acción ofensiva. La priorización de sus objetivos estará orientado hacia el apoyo de los fuegos preparatorios de artillería y aviación, contra nuestras principales posiciones defensivas, reservas y Puestos de Comando. Una vez que las operaciones han comenzado, su esfuerzo se orientará a localizar y destruir las instalaciones y sistemas de C^2; intentando "quebrar" sistemáticamente, la habilidad de nuestros Comandantes tácticos para comandar y controlar sus tropas disponibles y sistemas de armas de apoyo. Su objetivo final será maximizar la degradación de nuestros sistemas de Comando, Control, Comunicaciones e Inteligencia (C^3 I).
f. Contra este accionar, nuestros Comandantes buscarán degradar o impedir que la habilidad de los Comandantes (Cmdtes) enemigos (enos) les permita conducir su acción o ataque tal como lo planearon, realizando a su vez un sistemático ataque sobre sus "nodos" y "enlaces de información" de sus sistemas de c^2, que apoyan su proceso de toma de decisiones.
g. La lucha por mantener la habilidad para comandar y controlar las fuerzas, al mismo tiempo que se intenta negarle esa misma habilidad al oponente, constituye la "Guerra de C^2".
h. La G-C^2 es la aplicación combativa de la G-I en operaciones militares. El objetivo de la G-C^2 es influir, negar información, degradar o destruir las

posibilidades de comando y control del adversario; mientras protegemos las nuestras contra tales acciones.

i. El planeamiento de la G-C^2 es conducido sobre todo el continuo operacional militar, desde época de paz hasta la culminación de las hostilidades. En el pasado, el principal objetivo del combate fue concentrar potencia combativa física y destructiva contra el personal y el equipamiento adversario, esto es, tanques, aeronaves, artillería y defensa aérea. Posteriormente a comienzos de la década de los 90's nuestro ejército incorpora la doctrina americana de la batalla aeroterrestre que incluía este pensamiento mediante el enlace de operaciones aéreas y terrestres para alcanzar profundidad y sincronización. Un parámetro consecuente de la doctrina de la batalla aeroterrestre fue la intención de golpear a las reservas, los refuerzos y fuerzas del segundo escalón. Actualmente a la luz de la experiencia de las guerras y conflictos de los últimos 10 años, la estrategia operacional se ha extendido a las operaciones en profundidad con armas de largo alcance y operaciones de fuerzas especiales; buscando objetivos de alto valor con una estrategia orientada a la destrucción, degradación, negación y dislocación de nodos de C^2 críticos como uno de sus objetivos principales.

j. La guerra de C^2 en las operaciones de combate aeroterrestre son complejas, cuando se ven como un cúmulo de Telemática electrónicas cruzando en todas direcciones el campo de batalla. Sin embargo esta forma de guerra C^2, puede reducirse a términos de referencia más simples y extendibles, cuando se le ve como acciones o actividades tangibles e intangibles. Las actividades o acciones tangibles, son los "nodos" de Comando, Control y Comunicaciones (C^3), que presentan peculiaridades visuales a los Comandantes para verlos y dispararles. Las intangibles son los "Enlaces de Información" entre los nodos, que pueden interceptarse, identificarse y perturbarse.

k. La G-C^2 está definida como el empleo integrado de la SEGOPE, la GE, el engaño militar, las opns sicológicas y la destrucción física; apoyados mutuamente por la inteligencia; para negar info, influir, degradar o destruir las capacidades de C^2 adversaria; mientras protegemos las capacidades de C^2 amigo contra tales acciones. La G-C^2 se aplica a través del contínuo operacional y en todos los niveles del conflicto.

l. A nivel ejército, la G-C^2 dirige su apoyo al objetivo de alcanzar el dominio de la información y ganar cualquier guerra, conflicto o subsiguientes en cualquier opn de no-guerra, rápida, decisivamente y con el mínimo de bajas. La G-C^2 incorpora el concepto de "espada y escudo" empleado en la GE; el escudo contra las acciones de atq'- C^2 del adversario y la espada contra los sistemas de C^2 adversario. Esta combinación de aspectos ofensivos y defensivos en una capacidad integrada proporciona oportunidades expandidas para la sinergía en la guerra. La G-C^2 permite al ejército y cmdtes individualmente cumplir sus misiones con pocos riesgos, en marcos de tiempo más cortos y con menos recursos. El aspecto ofensivo de la G-C^2 puede hacer lento el ritmo operacional adversario, desarticular sus planes y habilidad para enfocar su potencia combativa; e influir su apreciación de la situación. El aspecto defensivo de la G-C^2 minimiza las vulnerabilidades del sistema de C^2 amigo y la interferencia mutua.

m. Estos aspectos ofensivo y defensivo de la G-C^2 constituyen sus componentes principales denominados: ataque de comando y control (Atq´-C^2) y protección de comando y control (Prot- C^2):
   (1) Atq´-C^2
      (a) El objetivo de la G-C^2 ofensiva o ataque de C^2, es ganar el control sobre las funciones de C^2 del adversario, tanto en términos de flujo de información como en nivel de conciencia situacional. Con un efectivo ataque de C^2, se podrá tanto prevenirse de un adversario por el ejercicio efectivo de nuestro C^2 o nivelándolo o apalancándolo a nuestro favor o ventaja.
      (b) El ataque-C^2 puede golpear las posibilidades adversarias en todos los escalones, tomando como objetivos al personal, equipo, comunicaciones y facilidades, en un esfuerzo para dislocar o darle la forma que deseáramos al C^2 adversario.
      (c) La información relevante e inteligencia (IRI) juegan un rol clave en el ataque-C^2 con la creación y mantenimiento de bases de datos en cada región militar sobre personal, sobre influencias históricas y culturales, preparación de inteligencia del campo de batalla (PIC) y evaluación de daños de batalla. El problema principal del atq´-C^2 para influir sobre el C^2 adversario es la aplicación sincronizada de las seis actividades de la información (obtención, empleo, explotación, negación, manejo y protección de la información y SINFOR).
   (2) Prot-C^2
      (a) Las operaciones de protección-C^2 buscan mantener un comando y control efectivo de las fuerzas amigas mediante la negación o tornándola en ventaja amiga de los esfuerzos adversarios; para influir, degradar o destruir los sistemas de C^2 amigo.
      (b) La protección -C^2 esta dividido en medidas activas y pasivas que buscan limitar las vulnerabilidades de las fuerzas (en personal, equipo e información) a la acción hostil, aún cuando las fuerzas desplegadas enfrentan amenazas sobre-expandidas y posibilidades adversarios.
      (c) La protección-C^2 incluye contrarrestar la propaganda adversaria para impedir que puedan afectar las operaciones amigas, sus opciones, la opinión pública y la moral de las propias fuerzas.

n. La complejidad y el alcance del AIM de hoy, incrementa la dificultad de alcanzar una desorganización, desarticulación y/o dislocación comprensiva de las posibilidades de C^2 adversario mediante algún ataque singular o aplicación del poder de combate. Esto realza la importancia de una efectiva integración y sincronización de los cinco elementos de la G-C^2: la guerra electrónica, el engaño, las operaciones sicológicas, la SEGOPE y la destrucción física; para lograr resultados máximos cuando se lancen ataques. Muy probablemente también se requerirá de una cuidadosa integración y sincronización para una total protección de nuestros SINFOR e inteligencia críticos, contra los ataques del adversario. Sin la completa y total integración de los cinco elementos de la G-C^2 en las dos disciplinas o componentes de la misma, la eficiencia operacional será reducida y las potenciales vulnerabilidades expuestas al eno.

96. PROTECCION DE COMANDO Y CONTROL (Prot-C^2)

a. Definición.- La protección-C^2 está definida como el mantenimiento de un C^2 efectivo de nuestras propias fuerzas convirtiéndolo en ventaja amiga o neutralizando los esfuerzos adversarios por negarnos info, o para destruir, degradar o influir el sistema de C^2 amigo.

b. Principios.-

(1) La protección–C^2 puede ser ofensivo o defensivo. En el primer caso usa los cinco (05) elementos de la G-C^2 para reducir la habilidad adversaria para conducir su atq'-C^2, y en el segundo caso reduce las vulnerabilidades de C^2 amigas al atq´-C^2 adversario mediante el empleo de una protección adecuada física, electrónica y de inteligencia.

(2) Este doble aspecto de la protección de C^2 hace que para entender su proceso, el cmdte deba preguntarse ¿cómo el adversario podría emplear sus opns de destrucción de GE, de engaño, de SEGOPE y Opns/Sicolog? para trastornar nuestros sistemas de C^2 y proceso de toma de decisiones. Haciendo un juego de guerra con las formas de acción de atq´-C^2 adversario, el cmdte puede desarrollar una opn de protección comprensiva sincronizada con el esfuerzo principal y con el propio ataque–C^2.

(3) De acuerdo a lo establecido en los sub-párrafos precedentes, el cmdte guiará sus opns de protección–C^2 con los principios sgtes:

(a) Ganar la superioridad de C^2.- Esto incluye funciones tales como procesamiento de info amigo continuo, desarrollo de formas de acción precisas, toma de decisiones válidas y comunicaciones eficientes hacia y desde los subordinados.

(b) Permanecer dentro del ciclo de decisión adversario.- Esto es hecho mediante la negación, influencia, degradación y/o destrucción de los sistemas de C^2 adversario; así como de su personal y equipos (Ver Manual de Empleo Táctico de GE párrafos 3 al 6 Ed 1998).

(c) Reducir la habilidad adversaria para conducir su atq´-C^2.

(d) Reducir las vulnerabilidades de C^2 amigas empleando medidas de protección de C^2, como por ejemplo contrarrestar los efectos de la propaganda o malinformación adversaria, mediante las tareas críticas de los recursos de GE para proteger el C^3 amigo (Ver párrafo 6 del manual de Seg de Com Ed 1998).

(e) Reducir la interferencia mutua de nuestros sistemas de C^3 mediante la administración del espectro electromagnético.

c. Efectos.-

(1) Los efectos de la protección de C^2 reflejan aquellos del atq´ - C^2; ya que podemos negar info que el adversario necesita para tomar una acción efectiva, podemos influir sobre el adversario para que no tome ninguna acción, tome una acción incorrecta o tome una acción en un momento no oportuno. También podemos degradar y destruir sus capacidades para realizar su atq´-C^2 contra fuerzas amigas.

(2) Las opns/sicolog y las opns de RP apoyan a la protección de C^2. La primera puede abrir una brecha ente el liderazgo adversario y su población para debilitar la confianza y efectividad del liderazgo adversario; las opns de RP a través de un "programa de info interno del cmdte" pueden beneficiar poderosamente para contrarrestar la

propaganda adversaria contra el país y fuerzas nacionales desplegadas, así como trabajando coordinadamente con personal especialista de inteligencia y de opns/sicolog se puede proteger a las tropas preparando productos que pueda emplear el cmdte contra los efectos de la desinformación y malinformación adversaria.

SECCION II. AMENAZAS A LA INFRAESTRUCTURA DE INFORMACION

97. CONSIDERACIONES SOBRE LAS AMENAZAS

a. Las amenazas a la infraestructura de información son genuinas, globales en origen, técnicamente multifacéticas y en crecimiento, que pueden provenir de individuos y/o grupos motivados por razones militares, políticas, sociales, culturales, étnicas, religiosas, personales, económicas e industriales; que perturban, alteran, hurtan, manipulan o destruyen los sistemas de información (SINFOR); sea para amenazar o simplemente para demostrar su habilidad.
b. Los perpetradores de tales amenazas tienen motivos diferentes para penetrar a los computadores, redes y sistemas. Algunos sólo buscarán entretenerse o distraerse, hurtando datos interesantes para retar a alguien más que use computadores o para competir con otro pirata; aunque curiosos, ellos no son activamente peligrosos, pero algunas veces pueden inadvertidamente causar daño a los sistemas. Otros perpetradores son atacantes o vándalos del computador, quienes deliberadamente buscan causar daños a organizaciones particulares y lo realizan así para asegurarse que el adversario conoce de su ataque. Finalmente hay un grupo de perpetradores o intrusos que son ladrones profesionales y espías quienes buscan robar y copiar datos sin dejar huellas o daño; que a menudo debido a la sofisticación de las herramientas que emplean sus ataques, no serán detectados.
c. La globalización de las redes de comunicaciones han creado vulnerabilidades debido al creciente acceso a la infraestructura de información desde diferentes puntos alrededor del mundo. Las amenazas contra las computadoras, sistemas de información del campo de batalla, sistemas de información automatizados (SIA´s), redes y sistemas de comunicaciones varían por: el nivel de hostilidad (paz, conflicto o guerra) las posibilidades técnicas y la motivación del perpetrador.
d. Los atacantes, los intrusos y/o los perpetradores comprometen las misiones, degradan a las redes y sistemas y en algunos casos destruyen las aplicaciones de hardware y software. Todo esto dificulta la efectividad de las fuerzas de apoyo y del cmdte apoyado. Virtualmente, es imposible defender todas las vulnerabilidades que pudiera experimentar nuestra infraestructura de información y procesos de información; sin embargo el desarrollo de programas de seguridad de SINFOR y protección de la información asegurarán que la protección necesaria y mecanismos de defensa estén en su lugar para ayudar en la protección de estas vulnerabilidades.

98. CATEGORIAS DE LAS AMENAZAS A LA INFRAESTRUCTURA DE LA INFORMACION

a. Las amenazas a la infraestructura de la información generalmente son divididas en las tres categorías siguientes:
   (1) Intencional
   (2) No-intencional
   (3) Ambiental

b. Intencional
   (1) Una intromisión intencional en las redes y sistemas, es un acto deliberado, considerados en muchos casos como delitos, contra los cuales se debe proteger, detectar y reaccionar. Las principales fuentes de amenaza en esta categoría son:
      (a) Usuarios no autorizados
      (b) Infiltrados
      (c) Terroristas
      (d) Grupos o activistas no gubernamentales
      (e) Servicios de inteligencia foráneos
      (f) Militares o políticos opuestos
   (2) Usuarios no autorizados, tales como los piratas, son la fuente que más ataca a los SINFOR en tiempo de paz. Aunque a la fecha, ellos han atacado principalmente a computadores personales; la amenaza que tienen a las redes y computadores tipo mainframe es creciente.
   (3) Insiders (infiltrados), son los individuos con acceso legítimo a un sistema o información confidencial. Cuando dichos individuos son reclutados o automotivados por cualquier organización o razón contraria a la organización a que pertenece, se convierten en la amenaza más difícil de la cual defenderse, ya que precisamente ellos conocen cual es la forma de protegerse contra ese ataque. Aunque un insider (infiltrado) pueda atacar un sistema en casi cualquier momento durante su período de vida (del sistema), los períodos de mayor vulnerabilidad para un sistema son durante su diseño, su producción, su transporte y su mantenimiento.
   (4) Terroristas, son aquellos cuyas acciones van desde el acceso no autorizado a una red de información hasta el ataque directo contra la infraestructura (con bombas). Se han identificado también grupos terroristas que usando computadoras anuncian pasar inteligencia y datos técnicos a través de fronteras internacionales.
   (5) Grupos o activistas no gubernamentales, son los nuevos actores, que van desde los carteles de drogas hasta activistas sociales, que toman ventaja de las posibilidades ofrecidas por la era de la información. Ellos pueden adquirir, a bajo costo, las posibilidades para golpear las infraestructuras de comunicaciones y de seguridad de sus enemigos comerciales, políticos, sociales, policiales, etc. Más aún, ellos pueden atacar con relativa impunidad desde distancias alejadas a sus objetivos, así como emplear los medios de comunicación internacional para intentar influir en la opinión pública global y formar percepciones de un conflicto; o pueden inflamar asuntos o temas dormidos, latentes u olvidados para que se conviertan en conflictos, que de otra manera no surgirían.
   (6) Servicios de Inteligencia foráneos, que están activos durante los períodos de paz y conflicto, tomando ventaja de la oferta anónima por

computador para ocultar su organización de búsqueda y reunión o para desorganizar actividades del oponente protegidos por la fachada de piratas no organizados. Sus principales objetivos a menudo son redes comerciales, científicas y de universidades, así como el ataque directo contra redes y sistemas militares y de gobierno.

(7) Militares o Políticos opuestos.- Aunque las actividades de estas fuentes están tradicionalmente más asociados con conflictos abiertos o guerra, su manipulación de medios de comunicación durante tiempo de paz pueden ayudarlos a enmarcar la situación a sus intereses o para su ventaja antes que se inicien las hostilidades.

c. No-intencional

(1) Una intromisión no-intencional en las redes, sistemas y computadoras ocurre más a menudo de lo que uno pudiera pensar o darse cuenta; ya que en muchos casos el propio intruso no tiene conciencia que ha ingresado a una red, aparato o sistema restringido. Esta categoría cubre a las fuentes siguientes:

(a) Infiltraciones abusivas.
(b) Torpezas de operadores y/o administradores.
(c) Contaminaciones de hardware y software.

(2) Infiltraciones abusivas.- El mal uso de redes y sistemas es un problema que concierne a todas las dependencias militares. Los infiltrados a estas organizaciones mantienen ocupadas a sus redes y sistemas mediante el envío de cartas canalizadas, frivolidades y bromas en los correos electrónicos; escuchando a difusoras vía internet; y otros usos no autorizados.

(3) Torpezas de operadores y/o administradores.- Las torpezas de operadores y/o administradores de red pueden causar grandes estragos a una red. Esto normalmente ocurre cuando un comando o un código de acción es insertado erróneamente en la red o sistema activo y llega a ser una acción de tiempo real. Estos errores toman lugar durante el planeamiento de la red o en la etapa operacional. Otros eventos, tales como corte de cables, pueden traer consigo el desbaratamiento de las redes y sistemas.

(4) Contaminación de hardware y software.- La contaminación de aplicaciones de software y equipo de hardware ocurre durante el desarrollo, manufacturación, ensamblaje y/o actualización/repotenciación de algún producto. Esto es diferente al ingreso de virus o bombas lógicas, que son actos intencionales.

d. Ambiental

El corte de fluido eléctrico, pérdida de energía en los sistemas, interferencia electromagnética, fuertes vientos, tormentas eléctricas y/o alta humedad; pueden constituirse en amenazas mediante la corrupción de los datos, destrucción física de los equipos y propiedad; y causar la pérdida de los servicios como si fuera un ataque físico adversario.

99. TIPOS DE ATAQUE CONTRA COMPUTADORAS, REDES/SISTEMAS DE COMUNICACIONES Y LOS SISTEMAS DE INFORMACION

a. Algunos ataques contra los sistemas de información (SINFOR), computadores, redes y sistemas de comunicaciones; tendrán un efecto retardado y otros se harán evidentes de manera inmediata; pero en ambos casos el resultado final será la corrupción de la base de datos o programas

de control, pudiendo degradar o destruir físicamente a estos elementos. Estos ataques pueden clasificarse en los tipos siguientes:

(1) Ataques a computadoras
(2) Ataques físicos
(3) Robos sistemáticos
(4) Ataques electrónicos
(5) Ataques de alta energía

b. Ataques a computadoras

(1) Los ataques a computadoras generalmente tienen como objetivo o propósito al software o datos contenidos en el computador del usuario final o en el computador de la infraestructura de red. Lo que busca el adversario es accesar a la información a la que no está autorizado pero de manera discreta para realizar modificaciones no-autorizadas al software y/o datos; o para destruir totalmente ese software y/o datos. Estas actividades pueden tener como blanco algún computador en particular o un gran número de computadores conectados a una LAN o WAN.

(2) Los ataques a computadoras pueden tener lugar durante las operaciones militares y pueden estar multifaceteados para dislocar/alterar las principales misiones militares. Estos ataques pueden ser parte de un esfuerzo mayor de alguna amenaza contra la infraestructura de información nacional y/o militar, tanto durante época de paz como de guerra.

(3) Los ataques a computadoras pueden envolver copia de archivos no autorizados, supresión directa de archivos, o introducción de software o datos maliciosos. Este último caso, generalmente es un código de software ejecutable introducido secretamente en un computador e incluye virus, “caballo de troya”, antivirus y puertas con trampas; entre otras formas.

c. Ataques físicos

(1) Los ataques físicos generalmente impiden la operación de los SINFOR y de las redes y sistemas de comunicaciones; al envolver la destrucción, daño, sobrecarga o captura de componentes del sistema. Esto puede incluir a los computadores de los usuarios finales, aparatos de comunicaciones y a los componentes de la infraestructura de red. Los ataques físicos que envuelven la sobrecarga y captura, permitirá al adversario emplear un ataque al computador.

(2) Estos ataques físicos pueden ser:
  (a) Sabotaje por cualquier medio
  (b) Ataques con armas de pequeño calibre
  (c) Ataques con armas automáticas
  (d) Ataques con tanques
  (e) Ataques con cohetes o misiles guiados
  (f) Ataques con artillería
  (g) Cualquier otro tipo que provoque destrucción, daño, sobrecarga o captura.

d. Robos sistemáticos

Un robo sistemático es una forma de ataque físico que no envuelve destrucción o daño, particularmente cuando está orientado al robo de artículos o elementos tales como claves criptográficas y/o passwords, que

más adelante podrían emplearse para apoyar un subsiguiente ataque al computador o ataque electrónico.

e. Ataques electrónicos
   (1) Los ataques electrónicos se centran sobre objetivos específicos o múltiples dentro de un área amplia. Los ataques contra los enlaces de comunicaciones incluyen a dos tipos de opns de inteligencia de Telemática (INTESE): interceptación y radiolocalización (Ver Cap 2, Sec I Párrafo 29 del TE 11-83, Seguridad de Comunicaciones).
   (2) La perturbación es otra forma de ataque electrónico contra los enlaces de comunicaciones.

f. Ataques de alta energía
   Los ataques de alta energía buscan como meta final sobrecargar a los componentes internos de un computador o red conduciendo energía directa a los circuitos electrónicos y/o de comunicaciones para dañarlos y dejarlos inoperativos. Se emplean generadores de pulsos electromagnéticos para tal fin.

SECCION III. SEGURIDAD DE LOS SISTEMAS DE INFORMACION

100. RIESGOS CONTRA LA SEGURIDAD DE LOS SINFOR

a. En el presente y en los próximos años nuestro ejército viene sobreincrementando su dependencia en los SINFOR automatizados; esto hace que la seguridad de la información (SEGINFOR) y de los SINFOR llegue a ser crítica. Desde época de paz hasta durante una guerra, las redes y sistemas a base de computadoras serán empleadas para procesar y transferir datos sobre logística, personal, administración, mantenimiento, finanzas y otras funciones de combate y apoyo de combate; que podrían ser vulnerables a un ataque.

b. La seguridad de la información está definida como la protección contra el acceso no autorizado o modificación de la información; durante el almacenaje, procesamiento o tránsito; y contra la denegación de servicio a usuarios autorizados o la provisión de servicio a usuarios no autorizados, incluyendo aquellas medidas necesarias para detectar, documentar y contrarrestar tales amenazas. La seguridad de los SINFOR, está definida como una composición de medios para proteger los sistemas de telecomunicaciones y los SIA´s; y a la info que trasmiten y/o procesan.

c. A menudo, la internet será una plataforma de comunicaciones favorita para los intrusos, si es que la unidad está conectada a una red. Una vez que se ha obtenido el acceso a la red de comunicaciones y computador-servidor de alguna dependencia, pueden realizarse en ella una amplia variedad de métodos y técnicas para perturbar, influir o atacar al sistema. Algunos de los métodos más comunes incluyen:
   (1) Inserción de software malicioso a través de contratistas.
   (2) Seguimiento de los cambios del software de mantenimiento y actividades del sistema de opns.
   (3) Alternar los enlaces de acceso o rastrear las máquinas que atrapan info sobre el tráfico y “passwords”.

d. Estos intrusos pueden iniciar su acción durante época de paz o en cualquier momento de una opn. Es aun posible que un sistema militar especialmente los equipos de comunicaciones y computadoras que

emplean microprocesadores, podrían venir de fábrica con una "bomba lógica" interna o virus programado para manifestarse en ciertas circunstancias o momentos.

e. Todos los riesgos mencionados en los subpárrafos precedentes y otros contra la info y SINFOR, imponen que los procedimientos y medidas de seguridad deban buscar preservar las SINFOR tanto activa como pasivamente en su integridad, confidencialidad y funcionalidad. Estas necesidades de protección incluyen medidas en tiempo casi real que detecten intrusos y alteraciones, así como la respectiva reacción y contracción para restablecer los SINFOR que el cmdte necesita para apoyar su opn militar. Las tres principales medidas de seguridad que se emplean son:
   (1) Procedimientos para asegurar la calidad de redes, programas y sistemas.
   (2) Negar ingreso a personal no autorizado a las instalaciones.
   (3) Programas de protección

f. Todas estas medidas se seguridad deberían estar desarrolladas en un programa de seguridad de los sistemas de información (P-SSI); que considere responsabilidades para los usuarios de todas las redes y sistemas, desde el cmdte de la organización hasta el soldado que opere directamente un aparato de comunicaciones o medio de transferencia de info. Adicionalmente, el P-SSI requerirá de una estructura para la seguridad de los SINFOR, procedimientos y reglas para la seguridad del personal que opere y administre los SINFOR y procedimientos para combatir a los intrusos dentro de las redes y sistemas.

g. Deberán asimismo existir organizaciones y personal específico dentro de la estructura de SSI, para responder a los intrusos y atacantes de las redes y sistemas. Ellos trabajarán estrechamente con los usuarios para PROTEGER, DETECTAR Y REACCIONAR a la intromisión y/o ataque a nuestra infraestructura de información. Estas tres actividades constituyen el área de responsabilidad compartida para los programas de SSI y de protección de la info que serán tratadas en el párrafo 102.

101. ROLES Y RESPONSABILIDADES DENTRO DEL P-SSI

a. Comandantes
   (1) Los cmdtes tienen la responsabilidad total por la seguridad de las redes y sistemas, para lo cual seleccionan personal que pueda proporcionarle asesoramiento en la implementación de procedimientos de seguridad.
   (2) Operan los sistemas dentro de su comando de acuerdo a su POV y normas/directivas emanadas de su escalón superior.
   (3) Designan un administrador de la seguridad de los sistemas de información (ASSI)
   (4) Establecen procedimientos razonables para proteger los sistemas de info y los datos contra el compromiso, robos o daños.
   (5) Incluye a la SSI en los programas de entrenamiento de su organización.
   (6) Usa los SINFOR para su propósito intentado.

b. Administrador del Programa-SSI (A/P-SSI)
   (1) Al escalón TO y superiores debería nombrarse un administrador del programa de seguridad de los sistemas de información (A/P-SSI), bajo

la dirección y supervisión del C-6 (Comunicaciones u opns de Telemática), quien será responsable de establecer, administrar y evaluar la efectividad del programa SSI en su comando o actividad.

(2) En coordinación con su comando, los cmdtes subordinados y los G-6´s recomiendan la designación de un ASSI.

(3) Desarrolla la arquitectura de seguridad.

(4) Coordina y revisa conceptos operacionales, POV´s y acreditación de seguridad para los sistemas de C^2.

(5) Asegura que las certificaciones de los sistemas individuales estén completas.

c. Administrador de la seguridad de los sistemas de información (ASSI)

(1) En todos los niveles de comando, debe designarse a un ASSI para establecer e implementar el P-SSI para todos los SIA´s. Este administrador normalmente estará dentro de la sección G-6/S-6.

(2) Desarrolla conceptos operacionales de los sistemas, POV´s de seguridad y acreditación de seguridad.

(3) Conduce evaluación de riesgo de sistemas individuales para la operatividad de sus sistemas de info.

(4) Conduce entrenamiento de seguridad de sistemas específicos y programas de concientización de seguridad.

d. Oficial de Inteligencia (G-2/S-2)

(1) Identifica y evalúa la amenaza de la inteligencia extranjera / foránea hacia los recursos del comando.

(2) Administra el programa de seguridad de personal de acuerdo a normas y directivas emanadas de su elón sup.

(3) Asesora en la identificación de factores de amenaza.

(4) Coordina con todas las agencias / dependencias del sistema de inteligencia.

(5) Evalúa los incidentes de seguridad e implementa los procedimientos del informe.

e. G-6/S-6 (Oficial de Opns de Telemática)

(1) El G-6/S-6 tiene la responsabilidad total por la seguridad de la operación de los sistemas de información automatizados (SIA´s), para lo cual contará con un Oficial de Seguridad de los SINFOR (OSSI). Este puesto normalmente será ocupado por el oficial de automatización o el administrador de sistemas.

(2) El OSSI tendrá las responsabilidades sgtes:

(a) Preparar, distribuir y mantener planes, instrucciones, guías y POV´s para la seguridad de los sistemas de C^2.

(b) Asegurar que todos los sistemas tengan la certificación y acreditación aprobada (operacional o genérica) para operar en el nivel secreto.

(c) Coordinar con el G-2/S-2 para asegurar que los usuarios cuenten con las investigaciones de seguridad requeridas, las autorizaciones y la necesidad-para-conocer.

(d) Establecer e implementar un sistema para la emisión, protección y cambio de sistemas de passwords.

(e) Establecer los programas de entrenamiento de los SSI y de concientización.

(f) Administrar la interconectividad de sistemas a la red y monitorear, revisar y evaluar el impacto de los cambios sobre la seguridad; coordinando esto con ASSI.
(g) Evaluar la amenaza directa y vulnerabilidades, que posibiliten al cmdte analizar apropiadamente los riesgos a los SINFOR y sistemas interconectados.
(h) Proveer guía para asegurar la máxima protección contra el compromiso y robo de info sensitiva e impedir el mal uso de los SINFOR.
(i) Mantener un inventario exacto de todo el hardware y software de la organización y que él mismo esté de acuerdo con los cargos.
(j) Asegurar que los planes contingentes incorporen necesidades de SINFOR.
(k) Conducir inspecciones y revisiones periódicas para asegurar el cumplimiento del POV y otras políticas en opns y seguridad.
(l) Suspender parcial o totalmente las opns ante la detección de acciones que podrían afectar la seguridad.
(m) Asegurar que los SINFOR o workstation son operadas, mantenidas y aseguradas de acuerdo al POV y otras disposiciones del elón sup.

f. Oficial de Seguridad de red (OSR)
(1) El OSR asegura la interconexión segura de los SINFOR sobre una LAN.
(2) Es también dependiente del G-6/S-6.
(3) Controla el acceso a las LAN´s
(4) Monitorea las asignaciones a las LAN´s para asegurar que los sistemas cumplan con las políticas de seguridad y directivas aplicables.
(5) Ayuda al OSSI en la preparación, distribución y mantenimiento del POV de seguridad.
(6) Conduce la revisión de la evaluación de riesgo conjuntamente con el OSSI y el ASSI.
(7) Ayuda al OSSI en la evaluación del impacto de los cambios sobre la seguridad a la red, incluyendo interfaces con otras redes.
(8) Coordina y monitorea periódicamente el adoctrinamiento de seguridad y las sesiones de entrenamiento para el personal asignado a puestos de seguridad.
(9) Conduce el entrenamiento específico de seguridad para los usuarios, como sea requerido.
(10) Informa al OSSI de cualquier intento de obtener acceso no-autorizado a info sensitiva de defensa, de cualquier falla del sistema o de cualquier sospecha que podría revelar acceso no-autorizado.
(11) Se asegura que los usuarios estén conscientes de la necesidad de verificar las autorizaciones de seguridad antes de otorgar acceso privilegiado a los SINFOR.
(12) Provee control positivo de los SINFOR dentro del área de responsabilidad de los usuarios.

g. Usuarios
(1) Cada operador o usuario de algún equipo o sistema de transferencia de info es responsable por su seguridad inmediata y permanente.
(2) Asegurar la operatividad de sus sistemas y equipos.

(3) Asegurar que su terminal/equipo sea operado adecuadamente de acuerdo a los procedimientos y POV.
(4) Realizar las tareas u obligaciones/deberes conforme han sido dispuestas por el OSSI y OSR para asegurar la protección y seguridad de la red y sistema.
(5) Informar al administrador de sistemas y/o OSSI sobre cualquier violación de seguridad, intento por accesar a la red o sistema, fallas en el equipo/sistema o de cualquier sospecha de estos actos.

102. AREAS DE RESPONSABILIDAD COMPARTIDA

a. La SSI y la protección de C^2, mantendrán un efectivo C^2 de las fuerzas mediante el balanceo de las ventajas proporcionadas por la digitalización y la negación al adversario para que influya, degrade o destruya nuestros sistemas de C^2. El objetivo o meta final de estas dos actividades será la integración de:
   (1) Las operaciones de Telemática
   (2) La ingeniería técnica
   (3) Las disciplinas de seguridad (seguridad de las opns, seguridad de Telemática, seguridad del personal, seguridad física, seguridad de la info, etc).
   (4) La inteligencia (o contrainteligencia)
b. La integración de estas áreas permitirá asegurar la autenticidad, la validez, la integridad, la confidencialidad y la disponibilidad de la información en tres grandes áreas de responsabilidad compartida, convencionalmente denominadas medidas de protección, de detección y de reacción.
c. PROTECCION
   (1) La protección de la información será crítica para la habilidad militar de conducir operaciones; y, será de responsabilidad de los líderes; productores, procesadores y usuarios de la info.
   (2) La protección de la info se aplica a cualquier medio y forma incluyendo a las copias de papel (mensajes, facsímil, cartas/oficios, documentos en gral); info electrónica, magnética, de vídeo, de imagen, de voz, telegráfica; computadores y personal operador/usuario.
   (3) El proceso de protección de la info envuelve determinar el propósito de la protección basado en el valor de la info protegida y en los estándares de protección de la info. El proceso de protección debería reflejar los cambios del valor de la info durante cada fase operacional.
   (4) La protección de las redes y sistemas considera los aspectos siguientes:
      (a) Perímetro digital externo, que consiste de seguridad de comunicaciones (SEGUCOM), firewalls o listas de control para acceder/filtrar rutas, guardas de seguridad y cuando sea necesario aislamiento físico que sirva como una barrera a redes externas tales como NIPRNET (Nonclassified Internet Protocol Router NETwork).
      (b) Perímetro digital interno, que consiste de firewalls y/o filtros de rutas que sirven como barreras entre escalones y/o comunidades funcionales. Las barreras internas pueden también usar SEGUCOM y seguridad física (guardas de seguridad).

(c) Seguridad de la workstation local, que consiste de controles de acceso individual, capacidad para inspeccionar la configuración, herramientas de prot-C^2 y detección de intrusos; y procedimientos de seguridad.

(d) Vigilancia de redes y sistemas, que a través de centros de administración de redes y sistemas proporciona en tiempo casi real vigilancia a eventos de seguridad sospechosos para redes y sistemas e inician acciones defensivas iniciales para bloquear o contener el ataque para minimizar el impacto operacional.

(e) Infraestructura elástica y robusta, que contiene la arquitectura de daños de ataques y hace que estos sistemas y redes sean rápidamente reparables si son atacados. El criterio fundamental es que ningún ataque singular causará la falla de una función crítica y que ningún mecanismo único protegerá las funciones o sistemas críticos.

(5) La seguridad de los sistemas de información (SSI) sólo ocurre cuando un juego común de procedimientos prescritos y controles técnicos se aplican a todos los recursos conectados a una LAN de usuario común y sobre toda la WAN. La protección contra los intrusos dentro o vía una WAN debe empezar con un esfuerzo cooperativo de SSI entre todos los institutos y el sector defensa en su conjunto. La protección contra la intromisión en redes de computadoras amigas mediante la negación del acceso o entrada no autorizada a estos sistemas, será esencial para la protección de la red. El entrenamiento y cumplimiento de la SEGOPE por los administradores del sistema, los operadores y los usuarios serán las mejores medidas para combatir el compromiso de los sistemas.

(6) Los programas de SSI deberían ser “duros” contra los intentos de los intrusos para obtener info vital o daño al flujo de la info. Ningún plan de protección será perfecto y los recursos para restaurar/proteger serán limitados, por lo que los planes y órdenes de opns especificarán las prioridades de los esfuerzos de protección. Los firewalls y el software de detección de intrusos son ejemplos de sistemas duros.

(7) La información proporcionada sobre las páginas web del ejército serán de particular interés para propósitos de seguridad. Las orientaciones de SEGOPE para páginas WEB serán igual como para cualquier otra información. La SEGOPE permitirá al cmdte identificar acciones de los sistemas de inteligencia adversario y observar a los potenciales intrusos, proporcionando una conciencia de los potenciales indicadores amigos que los sistemas de inteligencia adversario podrían obtener. La SEGOPE identifica, selecciona y elimina (o reduce a un nivel aceptable) info que es sujeta a explotación por los adversarios.

(8) El planeamiento de la SEGOPE cuenta hoy en día con nuevos retos provenientes de las capacidades comerciales globales, incluyendo imágenes, posicionamiento y sistemas celulares que ofrecen acceso a los potenciales adversarios a un nivel de información sin precedentes contra las fuerzas amigas. Los medios de comunicación noticiosos y los usuarios de correos electrónicos (E-mail) complican la SEGOPE durante las opns militares; ya que la habilidad de estos para trasmitir info en tiempo real a una audiencia mundial podría ser una fuente

lucrativa de info para el adversario. Los planificadores de la SEGOPE, deberían trabajar estrechamente con personal de relaciones públicas, los cmdtes y administradores de seguridad para desarrollar los elementos esenciales de información amiga (EEIA). Todo lo concerniente a la SEGOPE está ampliamente desarrollado en el ME 11-83 (Seguridad de Comunicaciones) en los párrafos 8 al 22; sin embargo en el párrafo 103 de este manual se hace un breve resumen de ellos.

(9) La seguridad de la info (SEGINFOR) y la SSI serán críticas para los SINFOR dentro del ejército, pues los sistemas y redes basados en computadoras sobre las cuales se procesan y transfieren datos e info logística, de personal, administrativa, financiera-económica y otros; son vulnerables a un ataque. A menudo, la internet será una plataforma de comunicación favorita para los intrusos, quienes obtendrán acceso a las redes de comunicaciones y computadoras de las unidades conectadas a plataformas de redes y sistemas comerciales mediante una amplia variedad de métodos y técnicas. Las necesidades de protección deberán incluir medidas en tiempo casi real que detecte a esos intrusos y alteraciones, así como la respectiva reacción y contracción para restaurar los SINFOR.

(10) La exitosa conducción de las opns en la era de la info, requerirá accesar a la info disponible fuera de la Z/O. Las infraestructuras de la info ya no más seguirán las líneas de comando tradicional y los combatientes necesitarán acceso frecuente, instantáneo y confiable a la info dentro y fuera de la Z/O. La complejidad técnica de las infraestructuras de la info pueden inhibir la habilidad de los cmdtes para administrar la info disponible.

(11) Nuestra futura dependencia en la info y SINFOR traerá consigo la exposición de nuestras vulnerabilidades, que harán que nuestros esfuerzos se centren en las opns de info defensiva que ocurren dentro del contexto de cuatro procesos interrelacionados:
  (a) Protección del ambiente de info
  (b) Detección del ataque
  (c) Capacidad de restauración
  (d) Respuesta al ataque

(12) Finalmente la seguridad de Telemática (SEGUTE) será otro factor importante para la SEGINFOR y SSI, particularmente las funciones se seguridad de trasmisión (SEGTRAS), seguridad criptográfica y seguridad de emisión, componentes básicos de la SEGCOM (Seguridad de Comunicaciones). Todos estos aspectos son ampliamente tratados en los capítulos 3 y 4 del ME 11-83 (Seguridad de Comunicaciones, Ed 1998), sin embargo en el párrafo 105 de este manual se presenta un breve resumen.

d. <u>Detección</u>

(1) Las facilidades de la administración de redes y sistemas (ARS) pueden detectar las ocurrencias que constituyan violación de las políticas de seguridad. Los eventos seleccionados u ocurrencias (tales como números intentos de entrar al sistema dentro de un período específico) serán monitoreados usando herramientas de detección y protección convencional. Las <u>violaciones a las políticas de seguridad incluyen</u>:

(a) Violación de la integridad, que es una indicación que ha ocurrido una interrupción potencial en el flujo de info (tales como info ilegalmente modificada, insertada o borrada).
(b) Violación operacional, que es una indicación que un servicio solicitado no está disponible o tiene mal funcionamiento.

(2) Los operadores, administradores y/o usuarios del sistema deben entrenar en todos los aspectos de la SSI sobre los SIA´s que requieren operar y mantener; para detectar la posibilidad de abuso del sistema y coordinar con el OSSI. Un apropiado sistema de seguridad física detectará y minimizará el acceso no-autorizado y la inadvertida, maliciosa o no, modificación o destrucción de datos. Los sistemas de computadoras serán vulnerables a un ataque cuando:
(a) Usuarios inexpertos o sin entrenamiento violan accidentalmente las buenas prácticas de seguridad mediante la develación de sus passwords.
(b) Passwords débiles que fácilmente pueden deducirse o encontrarse.
(c) Debilidades o vulnerabilidades de seguridad identificadas que no se corrigen.

(3) Las amenazas maliciosas pueden ser diseñadas intencionalmente para desencadenar virus de computador, provocar ataques futuros o instalar software de programas que comprometen o dañan a la info y sistemas. Aunque los fabricantes diseñen sistemas con seguridad en mente y el personal siga los procedimientos apropiados, la administración de la seguridad en tiempo real y la detección de intrusos deberá ser una parte de las opns de rutina, debiendo tomarse medidas reactivas cuando ocurran problemas.

(4) La administración de la seguridad alertará al administrador de las redes y sistemas sobre los intentos de intromisión y le dará un amplio rango de mecanismos de respuesta, que pueden incluir entre otros:
(a) Software antivirus.
(b) Capacidad de limpieza de discos duros (mantenimiento lógico).
(c) Sistemas de detección de intrusos.
(d) Sistemas de generación de passwords seguros.
(e) Aparatos/equipos de encriptado de red en línea.
(f) Cambios de perímetros digitales interno y externo.
(g) Reconfiguraciones de firewalls, ruteadores y de guardas de seguridad.
(h) Reenrutamiento del tráfico.
(i) Cambios en los niveles de encriptado o reenclavado.
(j) Cambios en los passwords y autenticaciones.

e. Reacción

(1) El ejército debe tener la habilidad para: proteger a los sistemas basados en computadoras y redes de datos, así como a la info que ellos transfieren o almacenan; detectar cuando sucede una intromisión; reaccionar para solucionar el problema; y proporcionar info relevante para las opns de info. Esto incluye operar durante períodos de degradación debido al ataque hostil, o a fallas en algún componente.

(2) Para las medidas de seguridad, un usuario, operador y/o administrador debería seguir los pasos de emergencia sgtes:

(a) Informar sobre el incidente a su supervisor inmediato, a su cmdte y al OSSI.
(b) Seguir las políticas de incidentes de seguridad de red de acuerdo al POV.
(c) Restaurar cualquier dato destruido o comprometido con su capacidad de "backup" (reserva/archivo).
(d) Informar del incidente a otras dependencias que sean necesarias.

103. SEGURIDAD DE LAS OPERACIONES (SEGOPE)

a. Concepto de SEGOPE

La SEGOPE consiste de un conjunto de acciones o medidas tomadas por un Cmdte para negar información al eno sobre sus posibilidades e intenciones, así como sobre sus planes, conducción de operaciones y actividades, mediante la identificación, control y protección de los indicadores que se asocien con la información a negar. Se ejecuta a través del Proceso de SEGOPE.

b. Categorías de las medidas de SEGOPE
   (1) Medidas de contravigilancia
   (2) Contramedidas (CM)
   (3) Engaño

c. Programa de SEGOPE
   (1) El programa de SEGOPE es un proceso de naturaleza cíclica, que toma en consideración los cambios que se producen en la interrelación de nuestras vulnerabilidades con las posibilidades del enemigo.
   (2) Las posibilidades del enemigo se ven incrementadas cuando sus sistemas de inteligencia cuentan con apropiados y modernos recursos de búsqueda y obtención de información; por lo tanto los Cmdtes de nuestras fuerzas en todos los escalones deben tomar acciones específicas para minimizar la habilidad enemiga de emplear eficiente y eficazmente dichos recursos contra nosotros. Estas acciones específicas están contenidas en el Programa de SEGOPE del Comando, que incluye la aplicación coordinada de una variedad de medidas y procedimientos que conforman necesidades únicas para cada Unidad, misión y situación, denominadas CATEGORIAS.
   (3) El programa de SEGOPE se desarrolla a través del Proceso de SEGOPE.

d. Proceso de SEGOPE
   (1) Es una secuencia de pasos que busca organizar todas las acciones que envuelven al proceso de toma de decisiones, para dar al cmdte la seguridad necesaria para no verse sorprendido por el enemigo.
   (2) Comprende los pasos siguientes:
      (a) Identificar los elementos enemigos de búsqueda y reunión de info.
      (b) Identificar los perfiles de nuestras fzas y recomendar EEIA.
      (c) Identificar las vulnerabilidades de nuestras fuerzas.
      (d) Realizar análisis de riesgos y seleccionar EEIA.
      (e) Recomendar contramedidas (medidas de SEGOPE).
      (f) Seleccionar contramedidas.
      (g) Aplicar contramedidas.
      (h) Dirigir esfuerzos para monitorear la efectividad de la aplicación de las CM.

(i) Monitorear la efectividad de las CM.
(j) Recomendar reajustes a las CM.

104. LA CONTRAINTELIGENCIA EN APOYO A LA SSI

a. Todas las actividades de CI pueden agruparse en tres (03) grandes núcleos: Contrainteligencia de Telemática, Contrainteligencia humana y Contrainteligencia de imágenes.

b. **Contrainteligencia humana**, son un conjunto de acciones que buscan vencer los intentos enemigos de usar fuentes humanas para buscar y reunir información tratando de neutralizar sus esfuerzos de espionaje, sabotaje y subversión.

c. **Contrainteligencia de Imágenes**, son aquellas que se toman para determinar las capacidades y actividades de la inteligencia de imágenes enemigas. Estas acciones incluyen: vigilancia de los sistemas de radar, fotográficos, térmicos e infrarrojos; evaluación de nuestras operaciones para identificar patrones y peculiaridades de imágenes; identificar las vulnerabilidades de las mismas y desarrollar y recomendar las contramedidas.

d. **Contrainteligencia de Telemática**
   (1) Son un conjunto de acciones que se toman para:
      (a) Determinar las capacidades, posibilidades y actividades de la INTESE y GE enemigas.
      (b) Apoyar nuestras operaciones mediante la identificación de patrones, perfiles y rasgos electromagnéticos.
      (c) Desarrollar y recomendar contramedidas.
      (d) Evaluar la efectividad de las contramedidas aplicadas.
   (2) Las contramedidas recomendadas para hacer frente a la amenaza enemiga incluyen activas u ofensivas y pasivas o defensivas tales como: perturbación electrónica, engaño electrónico, control de emisión (CONEM), apropiados procedimientos operacionales de radio, apropiados procedimientos de instalación de emisores; etc.
   (3) Las actividades de C-INTESE, a su vez se pueden agrupar en:
      (a) Técnicas de SEGUTE, que comprende dos grandes áreas: Seguridad de Comunicaciones y Seguridad Electrónica
      (b) Asesoramiento y asistencia a las COCOME.

e. El apoyo de la CI a la SEGOPE es también un proceso, que se concentra en desbaratar o degradar los esfuerzos multidisciplinarios de la inteligencia enemiga. El personal de CI deberá trabajar coordinada y estrechamente con la sección operaciones del EM (G-3), ayudándolo a desarrollar "perfiles" de nuestras fuerzas para compararlos con las posibilidades de la inteligencia enemiga. La comparación resulta en la identificación de nuestras vulnerabilidades que deben protegerse. La protección se efectúa desarrollándose CONTRAMEDIDAS que contrarresten los esfuerzos enemigos de su inteligencia humana, de imágenes y de Telemática, que amenacen a cada nivel o escalón.

f. Este apoyo se materializa mediante un proceso continuo que consta de cuatro pasos:
   (1) Evaluación de la amenaza
   (2) Evaluación de nuestras vulnerabilidades.
   (3) Desarrollo de las opciones de contramedidas.
   (4) Evaluación de la aplicación de contramedidas.

g. Consideraciones generales de contrainteligencia de Telemática
   (1) La C-INTESE, es una de las actividades de la CI, por lo tanto constituye también un proceso que enfatiza la necesidad de una fuerte aproximación analítica. La clave de ese proceso es ser "predictivo", basándose en el conocimiento del eno sobre sus posibilidades electromagnéticas y probables intenciones.
   (2) Conociendo las posibilidades e intenciones enemigas, entonces los planes y órdenes de nuestras fuerzas podrán adoptar medidas realísticas de seguridad.
   (3) La C-INTESE proporciona al Cmdte con el conocimiento de la evaluación de los riesgos electromagnéticos y probables éxitos de las alternativas antes que los planes puedan llevarse a cabo.

h. El proceso de contrainteligencia de Telemática consta de los pasos sgtes:
   (1) Evaluación de la amenaza electromagnética
   (2) Evaluación de nuestras vulnerabilidades electromagnéticas.
   (3) Desarrollo de las opciones de contramedidas
   (4) Evaluación de la aplicación de las contramedidas.

105. LA SEGURIDAD DE TELEMÁTICA EN APOYO A LA SSI

a. Concepto de seguridad de Telemática (SEGUTE)
   (1) Es un término genérico, que involucra una serie de medidas y/o actividades tanto de la Seguridad de las Operaciones (SEGOPE) como de la Contrainteligencia de Telemática (C-INTESE), destinadas a contrarrestar las actividades de Inteligencia de Telemática y de Guerra Electrónica del eno.
   (2) La SEGUTE busca la protección de la información operacional proveniente de nuestros emisores de comunicaciones y electrónicos, a través de la práctica de técnicas y tácticas de Seguridad de Comunicaciones (SEGCOM) y de Seguridad Electrónica (SEGELEC).

b. Funciones de apoyo de la SEGUTE
   (1) La SEGUTE se clasifica en una serie de funciones agrupados en dos áreas mayores denominados.
      (a) Seguridad de Comunicaciones (SEGCOM)
      (b) Seguridad Electrónica (SEGELEC)
   (2) La SEGCOM se subdivide a su vez en:
      (a) Seguridad física.
      (b) Seguridad Criptográfica.
      (c) Seguridad de Trasmisión.
      (d) Seguridad de Emisión.
   (3) La SEGELEC se subdivide a su vez en:
      (a) Seguridad Inherente
      (b) Seguridad Industrial
      (c) Seguridad Operacional

c. Evaluación de las vulnerabilidades de SEGUTE
   (1) Es una función de apoyo de la SEGUTE que se realiza para determinar hasta que punto los sistemas de emisores de comunicaciones y no-comunicaciones de nuestras fuerzas, así como sus radiaciones electromagnéticas, son susceptibles a ser explotados y/o desorganizados por el enemigo.

(2) Durante la ejecución de esta función se compara las posibilidades INTESE del enemigo, con los perfiles electromagnéticos de nuestras fuerzas, identificando las vulnerabilidades a la amenaza de colección enemiga. Una vez identificadas nuestras vulnerabilidades se deberá proporcionar el consiguiente asesoramiento en el desarrollo e implantación de contramedidas.

(3) El procedimiento para apreciar la vulnerabilidad electromagnética de una Unidad o actividad, se le conoce con el nombre de "evaluación de las vulnerabilidades electromagnéticas", la misma que comprende los pasos siguientes:

(a) Determinar rasgos, patrones y perfiles electromagnéticos.
(b) Identificar emisiones interrelacionados (discriminadores)
(c) Determinar las potenciales vulnerabilidades.
(d) Graficar trayectorias de trasmisión
(e) Identificar probables vulnerabilidades.

d. Seguridad de comunicaciones (SEGCOM)

(1) La SEGCOM es un conjunto de medidas, acciones y/o actividades destinadas a proteger nuestras telecomunicaciones; fundamentalmente negando a personas no autorizadas, información procedente de las mismas y/o evitando la interferencia, interceptación o engaño a nuestras redes de comunicaciones.

(2) La aplicación de las medidas de SEGCOM proporcionarán protección a través de los componentes esenciales sgtes:

(a) Seguridad física.
(b) Seguridad criptográfica.
(c) Seguridad de trasmisión.
(d) Seguridad de emisión (TEMPEST).

(3) Concepto de seguridad física de comunicaciones

(a) Es el componente de la SEGCOM que resulta de la aplicación de medios físicos para resguardar y/o proteger al material y a la documentación de SEGCOM, contra el acceso u observación por personal no autorizado.
(b) Estos medios físicos son controles que aseguran que el material y documentación de SEGCOM sean recibidos, empleados, archivados, transportados y destruidos de una manera segura.

(4) Concepto de seguridad criptográfica

(a) Es el componente de la Seguridad de Comunicaciones (SEGCOM) que resulta de la aplicación de sistemas criptográficos, técnicamente sólidos seguros y confiables, así como que éstos sean apropiadamente empleados.
(b) Se le conceptualiza también como el conjunto de medidas y procedimientos destinados a transformar el texto de un mensaje en claro en un texto ininteligible al monitoreo del eno.

(5) Concepto de seguridad de trasmisión

Es el componente de la SEGCOM, destinado a proteger la trasmisión durante el funcionamiento de los medios de telecomunicaciones de la interceptación, análisis de tráfico y contramedidas electrónicas (perturbación y engaño imitativo particularmente) que el eno podría efectuar con medios que no sean de criptoanálisis.

(6) Concepto de seguridad de emisión

(a) Es el cuarto componente de la SEGCOM, que resulta de tomar una serie de medidas para negar a personas no autorizadas, información de valor la cual podría ser obtenida de la interceptación y del análisis de emanaciones comprometedoras.

(b) El término en que los últimos años se viene asociando a tales esfuerzos es "TEMPEST" y/o control de emanaciones comprometedoras, ya que se refieren a la investigación y estudio de ellas. Normalmente, TEMPEST está orientado más a facilidades fijas y equipo electrónico que procesa información de alta clasificación.

SECCION IV. SEGURIDAD DE LA INFORMACION (SEGINFOR)

106. CONCEPTOS GENERALES SOBRE LA SEGINFOR

a. La SEGINFOR incluye la toma de medidas para prevenir (impedir), revelar, alterar, sustituir o destruir datos.

b. La operación segura de los sistemas de info requiere constante vigilancia y atención en un ambiente de constantes cambios. Los comandos y el personal administrador de la info, periódicamente debe reevaluar los riesgos de sus actuales ambientes operativos específicos en relación a la seguridad de los sistemas de información.

c. Para ayudar en la conducción de una revisión de seguridad de la información, algunas áreas específicas deberían reevaluarse sobre una base regular, tales como:

(1) Cumplimiento con la acreditación genérica.
(2) Administración del riesgo.
(3) Revisión de las violaciones de seguridad.
(4) Evaluación de los programas de entrenamiento de seguridad.
(5) Seguridad física de hardware y software.
(6) Seguridad de personal.
(7) Seguridad de recursos de automatización.
(8) Vulnerabilidades técnicas de automatización.

107. CUMPLIMIENTO CON LA ACREDITACION GENERICA

Los sistemas de info procesarán info clasificada en nivel SECRETO; por lo tanto los cmdtes y el personal de SSI serán responsables de consolidar los requerimientos de seguridad mínima de acreditación genérica de acuerdo a normas y directivas emanadas por su escalón superior; para lo cual pueden usar una lista de verificación de seguridad para determinar si sus organizaciones están cumpliendo con la acreditación genérica.

108. ADMINISTRACION DEL RIESGO DURANTE EL DESPLIEGUE DE SINFOR

a. El ME 11-30 (Opns y organización de EM de Comunicaciones/ Ed 1999) en su anexo 05 (Administración del riesgo) se detallan los aspectos principales sobre este tema. En este párrafo se ampliarán conceptos referidos a los sistemas de info, a la información y a la automatización en general cuando se despliegan los medios.

b. Todo el EM de la SSI comparten la responsabilidad por la operación apropiada de los sistemas de info. Cada sistema operacional del campo de

batalla (SOC) será responsable de conducir evaluación y revisión de la amenaza y de vulnerabilidad, la cual será una parte esencial del proceso de administración del riesgo. Los cmdtes locales y el personal de SSI deberán considerar el ambiente de seguridad en guarnición, en situaciones tácticas y en todos los ambientes operativos.

c. El despliegue de los sistemas de info debe estar acreditado para operar en tal ambiente. Un análisis de riesgo del sistema determinará el ambiente en el cual operará el sistema. Desde que las condiciones, incluyendo el ambiente y la amenaza, cambian conforme un sistema de computadoras se despliega, los factores siguientes deberán considerarse para el despliegue:
   (1) Sensibilidad.
   (2) Dependencia crítica.
   (3) Administración de password.
   (4) Seguridad Física.
   (5) Emanaciones de pulso electromagnético instantáneo estándar (TEMPEST: Transient Electromagnetic Pulse Emanations Standard).
   (6) Destrucción de emergencia.
   (7) Análisis de riesgo.
   (8) Planeamiento.
   (9) Requerimientos de back-up.

d. Sensibilidad
   La sensibilidad se relaciona a la info que se está procesando en una situación de despliegue y al nivel de clasificación del equipo o info que puede aumentar basado en la misión que apoya. Debería ser posible predecir el incremento de la sensibilidad antes del despliegue, mediante el estudio de evaluaciones de inteligencia y las órdenes de operaciones de la organización con la tarea de apoyo.

e. Dependencia crítica
   La dependencia crítica se relaciona a la misión del sistema de apoyo o al grado en el cual la misión depende del sistema. La dependencia crítica normalmente aumenta durante el despliegue debido al apoyo del comando del escalón superior y a los requerimientos operacionales de la misión. El usuario debe determinar que efecto podría tener la pérdida o alteración del sistema o datos sobre otros sistemas y misiones.

f. Administración de password
   El OSSI administra los passwords usados para el control de acceso de acuerdo a lo especificado en los reglamentos y directivas emanadas del escalón superior. Los usuarios no tendrán ningún control sobre la elección de sus passwords. Si los passwords son empleados para determinar la “necesidad-para-conocer”, la clasificación de ellos será al más alto nivel de info que puede accesarse.

g. Seguridad Física
   Las necesidades de seguridad física usualmente aumentan conforme la sensibilidad, la dependencia crítica y la amenaza aumentan. El OSSI determinará las medidas de seguridad apropiadas. La seguridad física será una parte importante de todo el plan de seguridad del computador durante las opns de despliegue, incluyendo el control del acceso a los computadores y el establecimiento de un perímetro seguro para el sitio de despliegue.

h. Destrucción de emergencia
El despliegue a un medio o áreas de alta amenaza dictará el desarrollo de procedimientos de destrucción de emergencia para el software, firmware, medio magnético, hardware y salida de copia dura (papel). El OSSI debe considerar el equipo usado, info procesada y la anticipación del tiempo disponible para la destrucción, empleando el mejor método posible.

i. Análisis de riesgo
El despliegue de sistemas requiere un paquete de análisis de riesgo. El OSSI conduce un análisis de riesgo del sistema para describir un ambiente de línea de base, el cual considere la protección mínima requerida para cada etapa de la opn. Las características de la seguridad del sistema debe satisfacer los requerimientos de seguridad para el ambiente más restrictivo.

j. Planeamiento
El OSSI ayuda al desarrollo de planes para el despliegue de los sistemas de info. Estos planes deben direccionar condiciones de despliegue operativo único, tales como variaciones de temperatura y humedad, fluctuaciones de energía, polvo, etc. Los planes necesarios para el despliegue incluyen un plan de seguridad y la continuidad del plan de opns. Este último debería considerar procedimientos de destrucción de emergencia y de clasificación, procedimientos de backup , fuentes de energía alterna, opn del sistema degradado o parcial, entre otros aspectos.

k. Requerimientos de backup
El OSSI investiga y documenta los requerimientos de los sistemas para un posible ambiente hostil y de mucha tensión. Estos requerimientos variarán con diferentes despliegues y sistemas de información, por lo que deberá considerar la tarea que está siendo automatizada, la dependencia crítica de la misión y el ambiente de despliegue. Igualmente, el OSSI debe considerar los factores humanos si es que se tendrá un back-up manual (o mecánico no automatizado). Los procedimientos para operar sistemas manuales y automatizados deberían ser similares, de tal forma que las transiciones puedan ocurrir rápidamente desde el modo automático al modo manual.

109. REVISION DE LAS VIOLACIONES DE SEGURIDAD Y EVALUACION DE PROGRAMAS DE ENTRENAMIENTO DE SEGURIDAD

a. La revisión de las violaciones de seguridad, debe hacerse de manera regular, incluyendo a todas las violaciones previas. El inspector, revisor o verificador intenta determinar si cualquier tendencia o patrón puede identificarse y que podría interesar como elemento de sospecha de violación. El resultado de este análisis debería ser incorporado en el programa de administración del riesgo y también ser un factor en la evaluación del programa de entrenamiento de seguridad.

b. Los programas de entrenamiento de seguridad deberían evaluarse periódicamente de acuerdo a las normas existentes, enfatizándose en los fundamentos de seguridad y en la emisión sobre sistemas de info.

110. SEGURIDAD FISICA DE HARDWARE Y SOFTWARE

a. El hardware, software, la documentación y los datos serán protegidos para impedir la revelación no autorizada, la destrucción, la negación de servicio o la modificación. La seguridad física es uno de los medios principales que se usan para protegerse contra estas amenazas.

b. La seguridad física en cada sitio está basado en un análisis de necesidades regulatorias, la dependencia crítica de la misión, la sensibilidad de los niveles de info que se procesa, las amenazas a la seguridad y la vulnerabilidad de los SINFOR a las amenzas.

c. Seguridad física durante el almacenaje y transporte

(1) En primer lugar, el usuario debe "purgar" todos los componentes de los SINFOR de acuerdo a los manuales técnicos aplicables antes del almacenaje o transporte, retirando todo el material clasificado y almacenándolo en contenedores especiales.

(2) Las necesidades por protección pueden aumentar durante el almacenaje o transporte debido a que aumenta la vulnerabilidad, lo que hará necesario incluir requerimientos especiales de manipuleo, tales como el control permanente del contenedor y tipo de protección a proveerse en el lugar de almacenaje.

(3) Después que todos los medios clasificados removibles se han retirado y que los no-removibles se han purgado, a los SINFOR se les debe proporcionar doble barrera de protección. Los componentes de los SINFOR normalmente serán almacenados en vehículos militares seguros o en cabinas de comunicaciones dentro de algún galpón con seguridad.

d. Seguridad física durante movimientos administrativos

(1) Antes de cualquier movimiento, todos los componentes de los SINFOR deben ser contabilizados y colocados en una configuración apropiada para ese movimiento de acuerdo a los manuales técnicos aplicables. Durante los movimientos administrativos, si el material clasificado está instalado sobre los componentes del SINFOR, un individuo autorizado deberá resguardarlos.

(2) Si fuese transportado por personal no-autorizado, el artículo criptográfico controlado deberá contar con doble barrera de protección durante el movimiento, tales como un cable de seguridad asegurando los componentes a la cabina y llave en la cabina; o desmontando los componentes y almacenándolos de manera separada para su transporte.

e. Seguridad física durante el movimiento táctico

Durante el movimiento, los SINFOR serán protegidos de acuerdo al nivel de clasificación de la info almacenada en ellos. El personal responsable, ejecutará los planes de destrucción de emergencia cuando sea inminente una emboscada, contacto con el eno o captura del SINFOR y/o componentes del mismo.

f. Seguridad física durante las opns tácticas

Durante las opns tácticas, los sistemas de info deben contar con un sitio seguro. Idealmente, el sitio tendrá una cerca perimétrica y guardia que limite el acceso de personal no-autorizado. La medida mínima es un guardia/centinela armado que provea seguridad al área. Los usuarios de los sistemas deben reforzar la disciplina de ruido y/o luces en el sitio para minimizar el riesgo de compromiso.

111. SEGURIDAD DE PERSONAL CON ACCESO A LOS SINFOR

a. Los cmdtes, los OSSI´s y los usuarios reforzarán los procedimientos se seguridad para limitar el acceso de personal no-autorizado. Los usuarios mantendrán un control positivo de los SINFOR durante todo momento,

incluyendo la restricción de personal no autorizado para observar las pantallas o monitores de los sistemas.

b. Necesidad-para-conocer
   (1) Todo el personal que opere los SINFOR de C^2 tendrán como mínimo una autorización de seguridad de clasificación SECRETA.
   (2) La cantidad de personal autorizado y acceso concedido a una red de C^2 será mantenido al mínimo. Ninguna persona tendrá acceso concedido simplemente porque posea el requisito de autorización de seguridad o debido al puesto de trabajo. Los cmdtes determinarán si una persona en posición individual necesitará acceso a la red de C^2. Solo el personal autorizado tendrá acceso a las áreas inmediatas donde están operando las computadoras.

112. SEGURIDAD DE RECURSOS DE AUTOMATIZACION

a. Todos los medios magnéticos removibles deberían llevar marcas externas que indiquen claramente la clasificación de la info que contiene.
b. Las impresoras de sistemas de C^2 inicialmente serán controladas como material secreto, conforme la situación operacional lo permita, el material será revisado para determinar su actual clasificación. Igualmente las cintas de impresoras y los cartuchos de toner/tinta tendrán marcas con el mismo nivel de clasificación conforme el material de impresión.
c. Seria ideal contar con trituradora de papel, en caso contrario se deben construir incineradores para la destrucción de no solo el material impreso, sino también de las cintas de impresoras, diskettes, masters, etc.
d. Cuando los componentes de los sistemas de info son almacenadas o dejados inatendidos toda la info clasificada debe removerse, purgarse, limpiarse, declasificarse y/o destruirse electrónicamente:
   (1) El primer componente a removerse será la memoria de acceso aleatorio (RAM: Random Access Memory), la cual es muy perecible y usualmente no accesible al usuario una vez que se ha retirado la energía. Sin embargo, los procedimientos de purgado establecidos en un POV deberán seguirse para asegurar que los datos clasificados se han removido.
   (2) El segundo componente ha removerse será aquel que tenga capacidad de almacenamiento permanente. La memoria de este componente usualmente no es afectado al removerse la energía, por lo que el POV deberá establecer los procedimientos para la protección apropiada de datos clasificados.
   (3) Purgar el medio significa borrar o sobreescribir total e inequivocamente cualquier info almacenada sobre el medio.
   (4) Limpiar el medio significa borrar o sobreescribir toda info sobre el medio, pero sin ser total y finalmente purgado, por lo que se deberá continuar controlando a su nivel de sensibilidad y clasificación.
   (5) Declasificar el medio se refiere a la acción administrativa que se toma después que se hizo el purgado, con la finalidad de reducir la cantidad de control y protección que se requiere. Si el medio contiene software o dato clasificado, copiarla y remover el medio si fuera posible.
   (6) Al menos que haya un aparato de hardware que impida escribir en el disco duro, clasificar y proteger éste al más alto nivel de clasificación de procesamiento hasta que sea purgado.

(7) Los SINFOR que tengan memoria de semiconductor no-volátil o no-removible no podrán purgarse. Si estos sistemas tienen procesada info clasificada, ellos serán protegidos como equipo clasificado.

113. SEGURIDAD DEL SOFTWARE

a. La seguridad del software dependerá de que tan rápido se identifica y resuelven los errores de software, los cuales por más insignificantes que parezcan deberían ser reportados para su investigación y corrección.
b. A pesar que los software puedan haberse probado intensivamente antes de su empleo en campaña, pudieran ocurrir algunos errores de software que podrían comprometer la seguridad; por lo que debe ser apropiadamente direccionado para preservar la protección que se le proporciona.
c. Los programas de entretenimiento (juegos) en disketts o CD´s son portadores ideales de virus y "caballos de troya"; ya que frecuentemente son copiados y ampliamente distribuidos; por lo que se deberá prohibir cargar este tipo de programas en los SINFOR militares o comerciales para uso militar.
d. Las trasmisiones sobre una LAN deben protegerse de la misma manera que las trasmisiones radiales, particularmente los protocolo y software de comunicación.
e. El G-6/S-6 y/o OSSI deberán asegurar que no se emplee software no autorizado, ni se copien software con restricciones de licencia sobre los SINFOR militar. De la misma manera deberá verificar que no se hagan modificaciones o alteraciones del software en uso para SINFOR, debiendo mantenerse la integridad del software.

114. SEGURIDAD DEL HARDWARE

a. De igual manera que el software, la seguridad del hardware dependerá de que tan rápido se identifique y resuelvan los errores del hardware.
b. El usuario será responsable de identificar el mal funcionamiento del equipo y ver si puede tomar alguna acción correctiva en el momento, para lo cual deberá verificar:
   (1) Que la energía y cable estén debidamente conectados.
   (2) Que todos los datos son correctos y que han sido ingresados apropiadamente
   (3) Que el "built-in-test (BIT)" sea monitoreado durante la inicialización del sistema.
   (4) Cualquier malfunción del equipo que afecte la seguridad
   (5) Que el manto local es conducido de acuerdo a los manuales técnicos y POV de unidad.
c. La seguridad del sistema es también dependiente de la instalación del arreglo del hardware, por lo que será crítico para la operación y la seguridad del sistema que los componente sean mantenidos en su configuración de instalación propia.

CAPITULO 7
SEXTA DISCIPLINA DEL APOYO DE TELEMÁTICA: GUERRA ELECTRONICA

SECCION I. INTRODUCCION A LA GUERRA ELECTRONICA

115. CONCEPTUALIZACION DE LA GUERRA ELECTRONICA

a. A la guerra electrónica (GE) se le ha definido y/o conceptualizado de muchas maneras, sin embargo la doctrina actual sobre la materia acepta que consiste en un conjunto de acciones militares que involucran al uso de energía electromagnética para determinar, explotar, reducir o impedir el uso hostil del espectro electromagnético; y, las acciones militares que propendan a la mejor utilización y control de ese espectro por nuestras propias fuerzas.

b. La GE explota, desorganiza y/o engaña los sistemas de comando, control y comunicaciones (C^3) del adversario, mientras protege el empleo de los sistemas de C^3 de nuestras fuerzas. Esta acción tiene un significativo efecto multiplicador cuando se integra y emplea con el fuego y la maniobra.

c. Actualmente la GE es un componente esencial de la guerra de comando y control (G-C^2) y como parte de ella, es empleada en conjunción con las múltiples disciplinas de contrainteligencia para la protección del C^2 amigo al mismo tiempo que ataca la estructura de C^2 enemigo. El empleo integrado de la GE con el esquema de maniobra del cmdte y con el plan de apoyo de fuego sobre todo el campo de batalla apoya la sinergia necesaria para localizar, identificar, dañar y destruir a las fuerzas enemigas y a su estructura de C^2.

116. COMPONENTES DE LA GUERRA ELECTRONICA

a. Actualmente a la GE se le reconocen tres componentes mayores:
   (1) Ataque electrónico (AE) antes conocido como contramedidas electrónicas (COME).
   (2) Apoyo de guerra electrónica (AGE) antes conocido como medidas de apoyo de guerra electrónica (MAGE).
   (3) Protección electrónica (PE) antes conocido como contra contramedidas electrónicas (COCOME).

b. Algunas acciones de GE son tanto ofensivas como de protección y pueden usar el AGE en su ejecución.

c. Ataque electrónico (AE)
   El AE es el empleo de energía electromagnética letal (energía dirigida) y no letal (perturbación y engaño) para desorganizar, dañar, destruir y eliminar fuerzas enemigas. Las unidades de GE usan AE no letal para perturbar el C^2 enemigo y sistemas de localización de objetivos, así como para apoyar a las operaciones sicológicas y a las operaciones de engaño.

d. Apoyo de guerra electrónica (AGE)
   El GE obtiene información mediante la interceptación, localización y explotación de las comunicaciones radioeléctricas enemigas y de sus emisores de no-comunicaciones (radares); proporcionando al cmdte con

info oportuna sobre la cual basará sus decisiones inmediatas. La inteligencia resultante del AGE apoyará al sistema de análisis de todas las fuentes, al AE y a la protección electrónica (PE).

e. Protección electrónica (PE)

La PE es la protección al personal, facilidades/instalaciones o al equipo de los efectos de la GE amiga o enemiga que pueda degradar o destruir nuestras capacidades de comunicaciones y no-comunicaciones. La práctica de buenas emanaciones electromagnéticas serán la clave para una defensa exitosa contra los intentos enemigos para destruir o interrumpir nuestros sistemas de comunicaciones y no-comunicaciones.

117. CLASIFICACION DE LA GUERRA ELECTRONICA

a. Actualmente a la GE se le reconocen tres componentes mayores:La GE se puede clasificar en:
   (1) Según su filosofía de empleo
   (2) Según sus componentes o actividad
   (3) Según sus estructura bélica
   (4) Según el sector del espectro electromagnético en que actúa.

b. Según su filosofía de empleo
   (1) Considerando que la GE es un proceso continuo y permanente de acciones militares, se infiere que sus actividades se llevan a cabo desde épocas de paz o períodos pre-operacionales, orientando su esfuerzo a la obtención de información mediante el reconocimiento del espectro electromagnético y/o tomar las medidas para evitar que el enemigo haga a su vez inteligencia sobre la forma como actúan nuestros sistemas electrónicos y de comunicaciones. Durante la guerra, además del apoyo a la inteligencia, la GE debe ejecutar acciones que busquen la anulación de los sistemas electrónicos y de comunicaciones enemigo, así como oponerse a los intentos del adversario por obstaculizar el uso efectivo del espectro por nuestras fuerzas.
   (2) Teniendo en cuenta lo expresado, la GE desde este punto de vista se puede clasificar en: Estratégica y Táctica.
   (3) GE Estratégica
      (a) Es llevado a cabo por los altos escalones de las Fuerzas Armadas y realizadas a grandes distancias para determinar esencialmente los planes de mediano y largo plazo del enemigo.
      (b) Esta GE es capaz de influir en acciones estratégicas y políticas, y se lleva a cabo en forma continuada todo el tiempo, en período pre-operacionales; lo que implica:
         1. Disponibilidad de tiempo
         2. Acciones a grandes distancias del potencial adversario
         3. Máximo empleo de acciones pasivas: Búsqueda, escucha, localización y análisis.
         4. Empleo de estaciones fijas y semifijas.
         5. Empleo de acciones activas, cuando la situación lo requiera: Perturbaciones de comunicaciones en casos excepcionales.
   (4) GE Táctica
      (a) Se realiza a niveles EO y GU, durante las operaciones y cerca del enemigo para facilitar el planeamiento para el combate táctico; lo que implica:

1. Tiempo relativamente corto
2. Acciones a cortas distancias del enemigo
3. Se emplean acciones pasivas y activas
4. Emplea unidades de GE altamente móviles y de gran autonomía

(b) El valor de GE Táctica radica principalmente en su capacidad para:
1 Proporcionar información esencial para tomar decisiones para el despliegue
2 Proporcionar conocimiento, en tiempo real, de las ubicaciones de las fuerzas enemigas.
3 Asesorar rápidamente para el planeamiento de operaciones de contra–ataque.
4 Optimizar el apoyo de fuegos (artillería, morteros, aviación).
5 Desorientar al enemigo mediante la perturbación de sus redes, sistemas de vigilancia y sistemas de armas.

c. Según sus componentes o actividad.- Pueden ser:
(1) Apoyo de GE o Medidas de apoyo a la Guerra Electrónica (MAGE)
(2) Ataque electrónico o Contramedidas Electrónicas (COME)
(3) Protección Electrónica o Contra Contramedidas Electrónicas (COCOME)

d. Según su Estructura Bélica
(1) Combate Electrónico
(a) Actividades de Reconocimiento (AGE), ya que básicamente se orienta a buscar información sobre los emisores electrónicos del adversario.
(b) Actividades Ofensivas (AE), ya que emplea acciones activas, destinadas a impedir el uso eficiente del espectro electromagnético por parte del enemigo.
(2) Defensa Electrónica o Actividades Defensivas (PE), ya que emplea técnicas y acciones, que buscan ocultar nuestro Orden de Batalla Electromagnético, de los intentos enemigos por determinarlo.

e. Según el Sector del Espectro Electromagnético.- Puede ser:
(1) Guerra Electrónica de Comunicaciones, que se realiza en la porción del espectro en que operan los Sistemas Radiales de Comunicaciones de HF, VHF, UHF y SHF, fundamentalmente.
(2) Guerra Electrónica de No-Comunicaciones, que se realiza en la porción del espectro en que operan los sistemas radiales de vigilancia, sensores remotos, sistemas electrónicos de guiados de cohetes, artillería, morteros y sistemas electrónicos de ayudas de navegación.

SECCION II. GENERALIDADES SOBRE LOS COMPONENTES DE LA GE

118. GENERALIDADES SOBRE EL APOYO DE GE (AGE)

a. Las actividades enemigas por conocer, deberán constituir una amenaza inmediata para el comandante táctico, ya que el AGE nos permite la búsqueda y localización de objetivos de combate electrónico, mediante la ESCUCHA y LOCALIZACIÓN de emisores electrónicos enemigos que

podrían afectar la operación en curso; y no necesariamente para relacionarla con otra información para inteligencia.

b. La idea del AGE es reunir datos e identificación que se requieren para evitar que el enemigo use con éxito sus propios sistemas de comunicaciones y electrónicos, tratando de determinar la magnitud de la fuerza e intenciones enemigas, así como informción necesaria para desorganizar los dispositivos electrónicos enemigos y actualizar el orden de batalla enemigo.

c. DE LA ESCUCHA DE LAS COMUNICACIONES ENEMIGAS OBTENEMOS:
   (1) Informaciones sobre sus sistemas electrónicos que nos sirven en la aplicación de medidas tendientes a reducir su eficacia de combate, al aplicársele perturbación. Simultáneamente podremos determinar sus posibilidades para perturbar nuestros sistemas, donde se encuentran sus perturbadores y en qué cantidad. Estas informaciones nos permitirá programar la destrucción del equipo de GE enemigo por nuestra artillería, Fuerza Aérea o Aviación del Ejército; para evitar que nos perturbe, protegiendo de esta manera nuestros equipos. Este accionar caracteriza a la GE como “lanza y escudo”.
   (2) Informaciones sobre dispositivos y actividades del enemigo que se destinan directamente al sistema de búsqueda para que sirva de inteligencia táctica. Por ejemplo, escuchando nos damos cuenta de que ha hecho su aparición en la zona de combate un aparato de radio con ciertas características técnicas y el asociarlo con cierto sistema de armas, se habrán adicionado datos al conocimiento sobre las posibilidades enemigas.

d. DE LA LOCALIZACIÓN DE UN EMISOR ENO OBTENEMOS:
   (1) Cuando está asociada a los datos técnicos del emisor localizado, informaciones para llevar a cabo operaciones de perturbación y de engaño electrónico contra el enemigo. El éxito de estas operaciones dependerá de la cantidad de información precisa, que se tenga sobre la ubicación del enemigo y de su equipo, habilidades, procedimientos, organización y posibilidades; lo que nos permitirá preparar un plan más eficaz, determinar la potencia, frecuencia y requisitos de señal para nuestros perturbadores, así como el lugar y la oportunidad de la operación. Por otro lado para realizar un engaño electrónico, se requerirá información sobre las características técnicas del equipo de Comunicaciones y Electrónica que emplea el enemigo, procedimientos de operación empleados, frecuencia de operación, tipo de señal, procedimientos de autenticación, técnicas radiales, etc.
   (2) Ubicación aproximada de las antenas de un radio o radar enemigo, que nos ayudará a determinar movimientos, dispositivos y acumulación de datos del objetivo.

e. La integración de las posibilidades de escucha y localización con la posibilidad tradicional de recursos fotográficos hoy llamado Información Visual; sensores infrarrojos, radar aerotransportado de búsqueda lateral y otros medios, pueden ofrecer al cmdte táctico una inteligencia de combate precisa, que le será de gran utilidad en su toma de decisiones.

f. El propósito principal del AGE es ubicar sensores con la suficiente precisión que permita conducir operaciones de ataque electrónico o aplicar protección electrónica. Sin embargo es muy difícil poner a disposición de

un cmdte táctico la suficiente cantidad de equipos y personal especialista para escuchar y localizar a cada uno de los sistemas electrónicos enemigos; por lo tanto será necesario dar prioridades, normalmente a Telemática enemigas asociadas al Comando y Control de la GU, elementos de Guerra Electrónica, artillería, cohetería y defensa antiaérea.

g. Cuando el AGE se integran con otro tipo de información o inteligencia, normalmente se puede dar respuesta a las preguntas "¿QUÉ?" y "¿DÓNDE?".

119. ATAQUE ELECTRONICO (AE)

a. El AE constituye una parte de la Guerra Electrónica (GE), específicamente del Combate Electrónico, que comprende un conjunto de acciones o actividades que se llevan a cabo para prevenir o reducir, la capacidad del enemigo para emplear eficazmente el espectro electromagnético, particularmente sus sistemas de comunicaciones, de vigilancia y de búsqueda y localización de objetivos.

b. El AE es un arma, pero su efecto es diferente al de las armas convencionales que pueden causar daño físico al enemigo. El AE no destruye, pero puede anular la acción del enemigo influyendo efectivamente en el resultado de las operaciones. Muchas veces la única indicación de la efectividad del AE será el resultado final de la acción.

120. TIPOS DE ACCIONES O ACTIVIDADES DEL AE

a. El AE puede clasificarse en tres tipos:
   (1) Perturbación electrónica
   (2) Engaño electrónico
   (3) Destrucción física del emisor-receptor electrónico

b. La perturbación y el engaño electrónico se explica ampliamente en manuales especiales, pero en los párrafos subsiguientes se hará un breve resumen de ellos. En los referente a la destrucción física del E-R electrónico, cabe mencionar que será una acción de ataque que se pondrá a la decisión del cmdte táctico, desde que la misión principal de la GE es negar al enemigo el uso completo de sus facilidades electrónicas; sin embargo, aunque esta acción pudiera ser considerada como la más óptima y positiva, será la más difícil de decidir y deberá ser más ampliamente coordinada y estudiada, porque los sistemas electrónicos enemigos, especialmente los de comunicaciones, de una u otra manera proporcionan información a ser explotada por la inteligencia u otras armas. La ejecución de esta acción deberá ser también coordinada con otras armas o fuerzas.

c. Cualquier equipo electrónico identificado y/o ubicado es vulnerable a cualquier acción del AE. El efecto inmediato esperado es la "desorganización" del equipo electrónico o de la red a la que pertenece, buscando anular cualquier acción eficaz del operador del equipo, hasta lograr la "destrucción electrónica" del mismo; es decir que no se pueda emplear o que se emplee de la manera que deseamos para favorecer a nuestras intenciones tácticas.

121. CONCEPTO DE PERTURBACION ELECTRONICA

a. Es la radiación, re-radiación o reflexión deliberada de la energía electromagnética, con el propósito de impedir u obstaculizar el empleo de los dispositivos, equipos o sistemas electrónicos
b. La radiación, se realiza empleando un equipo perturbador en la(s) frecuencia(s) a perturbar, sin alterar las Telemática. La re-radiación (o retrasmisión) se realiza cuando un receptor especial (activo) recibe las trasmisiones del emisor-objetivo, las alterna de alguna manera y luego re-radia la señal de regreso al mismo emisor-objetivo o a su receptor(es) asociados. La reflexión se realiza empleando elementos pasivos contra los sistemas de vigilancia y de búsqueda y localización de objetivos.
c. Lo que se busca con la perturbación electrónica es negar o al menos reducir la capacidad del receptor para recibir la información o el mensaje esperado.
d. De una manera general, se puede afirmar que cualquier tipo de radio con suficiente potencia y a la distancia adecuada puede perturbar a un receptor; sin embargo para GE se ha diseñado y fabricado equipos especiales, denominados PERTURBADORES.
e. Relación entre la perturbación y la interferencia
   (1) La perturbación y la interferencia constituyen emanaciones de energía electromagnética que más afectan o degradan a las comunicaciones y al funcionamiento normal de cualquier equipo electrónico receptor de Telemática. Sin embargo es muy frecuente que los operadores de los equipos confundan como si fueran del mismo origen.
   (2) La diferencia fundamental entre ambas emanaciones radica en que la perturbación electrónica siempre será deliberada o intencional, mientras que la interferencia puede deberse, además a causas espurias o fortuitas.
   (3) El saber distinguir si una interferencia es o no intencional corresponde al operador.
f. Finalidades de la perturbación
   Siendo la perturbación una acción deliberada o intencional, la decisión final de aplicar tal acción será el resultado de un proceso de planeamiento y toma de decisión. Decidida su aplicación, las finalidades que buscará la perturbación pueden ser:
   (1) Disminuir temporalmente la efectividad del equipo electrónico enemigo, ya sea bloqueando o sobresaturando el receptor con una señal potente.
   (2) Confundir al operador enemigo trasmitiendo Telemática que oculten o disimulen la información o imágenes que realmente debía recibir.
   (3) Afectar los sistemas de seguimiento, rastreo o escucha, enviando Telemática que tiendan a confundir dichos sistemas.
   (4) Engañar al operador de vigilancia de radio o radar, introduciéndole información o imágenes falsas en su auricular y/o pantalla.
g. Factores de eficacia de la perturbación
   (1) En general la eficacia de la perturbación depende de los factores siguientes:
      (a) Relación de potencias entre el trasmisor y el perturbador
      (b) Distancia entre el receptor – objetivo y el perturbador
      (c) Existencia de obstáculos o barreras en el terreno, en la línea de vista o visada entre el perturbador y el receptor-objetivo

(d) Empleo en el receptor-objetivo de una adecuada antena direccional
(e) Polarización de la antena
(f) Modulación y frecuencia del perturbador
(g) Ubicación adecuada del perturbador compatible con el receptor – objetivo.

(2) Para perturbar con eficacia a un receptor-objetivo situado a gran distancia, el perturbador debe aumentar la potencia de su señal proporcionalmente a esa distancia, para conseguir el mismo efecto, ya que la señal u onda terrestre es atenuada o debilitada conforme se desplaza por el terreno. Sin embargo, los perturbadores al igual que cualquier otro trasmisor, tiene un límite en su potencia, lo que puede superarse, en parte, empleando perturbadores aerotransportados que requieren de menos potencia para conseguir el efecto deseado, debido a su acción directa sobre el receptor (línea de vista).

(3) Si no es posible bloquear o cancelar completamente la recepción de un mensaje en el receptor, la trasmisión del mismo puede distorsionarse a tal punto de conseguir el mismo efecto, mediante la intromisión de una señal discordante de perturbación (por ejemplo: varias voces en el propio idioma enemigo, sonido de gaitas, rugidos, etc)

122. ENGAÑO ELECTRONICO (DECEPCION ELECTRONICA)

a. Se denomina engaño electrónico a las operaciones de radiación deliberada, re-radiación, alteración, absorción, intensificación o reflexión de la energía electromagnética; de tal manera, que intenta confundir o desorientar al enemigo en la interpretación o en el empleo de la información recibida por sus sistemas de comunicaciones y electrónicos.

b. Generalidades sobre el engaño electrónico (EE)

(1) El EE es empleado para causar en el enemigo la pérdida de la capacidad interpretativa de lo que recibe a través de sus sistemas de comunicaciones y electrónicos.

(2) Normalmente el EE, es conducido como parte de una operación más amplia de engaño, rara vez se realiza sólo. A nivel táctico, se integra, despliega y refuerza las operaciones de engaño táctico.

(3) El EE requiere un planeamiento y entrenamiento único y específico, así como ser bien controlado, si se desea que sea efectivo.

(4) El planeamiento y dirección de las operaciones de EE corresponde a los G-3´s, que estarán asesorados y/o coordinados por la Sección o negociado de planeamiento de Guerra Electrónica y por el G-6/S-6.

c. Categorías de las operaciones de engaño electrónico

(1) Engaño Electrónico Simulativo (EES)
(2) Engaño Electrónico Imitativo (EEI)
(3) Engaño Electrónico Manipulativo (EEM)

d. **Engaño Electrónico Simulativo (EES)**

(1) Concepto.- El EES consiste en la creación de emisiones electromagnéticas para representar posibilidades reales o imaginarias de nuestras fuerzas con la intención de confundir o inducir a error al enemigo, sobre nuestro dispositivo, composición y fuerza.

(2) Generalidades sobre el EES

(a) El EES busca enfrentarse a los esfuerzos de la GE enemiga y a su inteligencia de Telemática, mediante la simulación de unidades

existentes o posibilidades de las mismas, así como simulando unidades reales o sus posibilidades en ubicaciones falsas.

(b) El EES comprende acciones relacionadas con las radiaciones de nuestros equipos de comunicaciones y electrónicos. Estas acciones pueden ser ejecutadas por cualquier elemento presente en la zona de combate, empleándose sólo sus puestos de radio o equipos electrónicos.

(c) El Comandante de Comunicaciones desempeña el rol principal en el planeamiento y ejecución de esta categoría de EE.

(d) Tanto los equipos de Comunicaciones como los equipos electrónicos (que no son de comunicaciones), pueden emplearse en la simulación; dependiendo del tipo de engaño que será proyectado al enemigo.

e. **Engaño Electrónico Imitativo (EEI)**

(1) Concepto.- El EEI consiste en la introducción de radiaciones falsas y engañosas en los canales de comunicaciones y electrónicos enemigos, imitando sus emisiones como verdaderos o creíbles.

(2) Generalidades sobre el EEI

(a) El EEI busca ingresar a las redes de comunicaciones y electrónicas enemigas, como si fueran reales miembros de sus sistemas y una vez admitidos se mantienen en ellos hasta que una deseada información falsa sea cursada y aceptada por él.

(b) El EEI, comprende acciones relacionadas con las radiaciones de las fuerzas enemigas. Estas acciones deben ejecutarlas casi exclusivamente las unidades de GE de nuestras fuerzas, debido a que requiere técnicas especiales.

(c) Las operaciones de EEI, deben adoptar extremos cuidados durante la ejecución del proceso de ingreso a los sistemas de comunicaciones y electrónicos del enemigo, debido a cada emisor produce su propio particular patrón. Nuestros emisores de EEI deben aproximarse lo más cerca posible a ese particular patrón enemigo.

(d) Si nuestras operaciones de EEI son descubiertas, se le habrá proporcionado al enemigo una indicación del éxito de nuestra INTESE, consecuentemente incrementará sus esfuerzos de SEGUTE para impedir la interceptación y análisis de sus comunicaciones.

(e) El G-3, desempeña el rol principal en el planeamiento y ejecución de esta categoría de engaño.

f. **Engaño Electrónico Manipulativo (EEM)**

(1). Concepto.- El EEM consiste en la alteración de las características, patrones o procedimientos de nuestras emisiones electromagnéticas; para eliminar manifestaciones o dar informaciones engañosas, así como indicadores reveladores; que pudieran ser empleadas por el enemigo.

(2). Generalidades sobre el EEI

(a) El EEM busca tener a los analistas enemigos de AGE y de INTESE, aceptando un perfil de la información, manipulada intencionalmente, como válida; y, que con ella llegue a conclusiones erróneas de nuestras actividades e intenciones.

(b) El EEM, al igual que el EES, comprende acciones relacionadas con las radiaciones de nuestros equipos de comunicaciones y electrónicos. Igualmente pueden ser ejecutadas por cualquier elemento presente en la zona de combate.

(c) En esta categoría, G-6 apoyado por el Oficial de GE y el Cmdte de la Unidad de GE desempeña el rol principal en su planeamiento y ejecución.

(d) El EEM, es el que más comúnmente se puede emplear como parte del engaño táctico, aunque podría ser empleado como un acto aislado de engaño, pero por muy corto tiempo.

(e) El EEM, se constituye como un tipo de técnica protección electrónica pre-planeada.

(f) El tiempo es un elemento crítico de cualquier plan de EEM, por lo que si se planea engañar al enemigo por 2 o 3 días, entonces, el argumento a emplear en esta categoría, debe ser muy bien elaborado y coordinado, pues si el enemigo dispone de tiempo podrá analizar una suficiente cantidad de emisores que le pueden ayudar a descubrir el EEM. Sin embargo, si el contacto o enganche con el enemigo es inminente o ya ha ocurrido, el EEM por sí mismo podría significar para el Cmdte de la fuerza táctica, la ventaja necesaria para ganar el combate.

123. PROTECCION ELECTRONICA

a. La Defensa Electrónica, es también conocida como: Guerra Electrónica Defensiva o Protección Electrónica; y consiste de aquellas acciones tomadas para proteger y asegurar el uso efectivo de nuestros emisores en el espectro electromagnético, contra los esfuerzos del enemigo en la búsqueda y localización de sus objetivos de GE, así como contra la perturbación, el engaño electrónico y la destrucción física.

b. Los comandantes tácticos confían en sus emisores electrónicos y de comunicaciones para su comando y control, así como para muchas otras funciones críticas dentro del campo de batalla. La primera prioridad de la GE es proteger estos emisores de la detección, localización e identificación por parte del enemigo.

c. Los puestos de comando o los sistemas de armas no podrán supervivir en el moderno campo de batalla si ellos pueden ser localizados por causa de sus emisiones electromagnéticas. La supervivencia dependerá del desarrollo y uso de buenas tácticas y técnicas de protección electrónica, destinadas a reducir la eficacia del enemigo a la detección y localización; así como a la obtención de objetivos por su GE.

d. Consideraciones sobre la Protección Electrónica

(1) La PE son responsabilidad del Comando. Básicamente, todo Comandante debe asegurar que su Unidad esté entrenada para operar en un ambiente electrónico hostil.

(2) La PE son por naturaleza protectoras y/o preventivas.

(3) El planeamiento de la PE se basa en la misión y concepto de la operación del Cmdte. Este planeamiento comienza con la identificación de nuestros emisores esenciales y comunicaciones sensibles que deben ser protegidas. Luego se evalúan sus rasgos, peculiaridades, perfiles, características y patrones; comparando sus vulnerabilidades

contra las posibilidades del combate electrónico enemigo. Finalmente la PE es planeada para eliminar o reducir estas vulnerabilidades.

(4) Como se ha manifestado anteriormente la PE está muy estrechamente relacionada con la SEGUTE:
   (a) Ambas actividades son defensivas en esencia
   (b) Ambas se basan en el mismo principio: negar al enemigo acceso a nuestros elementos esenciales de información.
   (c) Ambas deben preplanearse y basarse en las AGE y AE y posibilidades de destrucción enemiga.
   (d) Mientras la SEGUTE están destinadas principalmente a darle confianza al Cmdte, asegurándole que cuando haga uso del espectro electromagnético no será explotado por el enemigo; la PE aseguran cierto grado de confianza en su uso continuo.
   (e) Un aumento en el empleo de las técnicas de SEGUTE reducirá la necesidad del empleo de ciertas medidas de PE. Por eso es que:
      1. Nuestro objetivo debe ser: asegurar que tanto las comunicaciones, los sistemas de vigilancia y de búsqueda y localización de objetivos, puedan ser empleados efectivamente por los Cmdtes tácticos a pesar de los esfuerzos del enemigo por degradarlos y sacar ventaja de ello. Es muy difícil, por lo altamente costoso, contar con todo el equipamiento electrónico con dispositivos internos de PE que lo haga menos susceptible a los esfuerzos de GE enemigos.
      2. La Seguridad de Telemática (SEGUTE) y la operación continua de todos los emisores, debe ser una preocupación permanente desde el cmdte hasta el último operador; y, esto se traduce en entrenamiento:
         a. A los operadores se les tiene que enseñar lo que la perturbación y el engaño electrónico pueden causar a las comunicaciones u otros sistemas electrónicos, si es que los emplean mal o no son capaces de reaccionar instintivamente para contrarrestarlo.
         b. Al personal de mantenimiento se le debe alertar de los riesgos de realizar reparaciones del equipo sin tomar las medidas de seguridad, así como de las consecuencias de efectuar modificaciones inapropiadas en los mismos, que podrían provocar la emisión de características peculiares fácilmente identificables por el enemigo.

(5) Las COCOME tienen como objetivo lo siguiente:
   (a) Reducción de la probabilidad de detección de las comunicaciones
   (b) Dificultar la utilización de los equipos de RL enemigos.
   (c) Discriminar la interferencia de la perturbación.
   (d) Evitar o reducir la perturbación enemiga.
   (e) Permitir conservar un objetivo adquirido (enganchado / traqueado)
   (f) Prevenir la saturación de equipos detectores o de identificación (por exceso de Telemática)
   (g) Discriminar blancos falsos.

CAPITULO 8
ADMINISTRACION DEL ESPECTRO RADIOELECTRICO

SECCION I. FUNDAMENTOS CONCEPTUALES SOBRE EL ESPECTRO RADIOELECTRICO Y ADMINISTRACION INTERNACIONAL DEL MISMO

124. EL ESPECTRO RADIOELECTRICO

a. El espectro radioeléctrico o el espectro de frecuencias radioeléctricas es una parte del espectro electromagnetico que incluye al conjunto de frecuencias comprendidas entre los 9 Kilohertzcios (Khz) y 3000 Gigahertzcos(Ghz), cuya utilización para aplicaciones de radiocomunicaciones está regulada por acuerdos internacionales, celebrados en el marco de la Unión Internacional de las Telecomunicaciones (UIT).

b. Esta regulación o administración del espectro radioeléctrico debe hacerse de manera internacional debido al hecho que, casi desde el mismo nacimiento de las radiocomunicaciones, los países se percataron de la imposibilidad práctica de hacer uso de aquellas técnicas sin una coordinación de la utilización de las diferentes frecuencias, en vista que el uso de una frecuencia en un lugar geográfico dado, impediría el uso de la misma frecuencia al mismo tiempo en un espacio más o menos grande en torno a aquel (dependiendo de las características de las emisiones), produciéndose en caso contrario interferencias o perturbaciones, que se afectarían mutuamente, impidiendo o menoscabando la trasmisión de la información requerida.

c. Lo expuesto en el subpárrafo anterior, unido a la necesidad de preservar la soberanía de los estados en el establecimiento de sus sistemas de radiocomunicaciones nacionales, han provocado el desarrollo del concepto de "Dominio Público Radioeléctrico", cuya definición más extendida es el "espacio físico por el que pueden propagarse las ondas radioeléctricos que forman el espectro radioeléctrico".

d. El hecho de que al espectro radioeléctrico se le considere un bien de dominio público tiene una fundamental importancia de naturaleza jurídica a la hora de reglamentar y ordenar su uso y ello en base a las características que, por su naturaleza, son consustanciales a todos los bienes de dominio público, esto es: su pertenencia al Estado, su inalienabilidad, su imprescriptibilidad e inembargabilidad.

e. Por otro lado, el hecho que hoy en día puedan establecerse una gran variedad y diversidad de servicios de radiocomunicaciones, cada uno de ellos con características técnicas a veces muy diferentes unos de otros y por lo tanto con diversos grados de incompatibilidad mutua, ha ido haciendo necesario ir efectuando particiones dentro del espectro radioeléctrico, y estableciendo un uso homogéneo de cada una de estas partes a nivel mundial y regional, atribuyendolas a uno o más servicios de radiocomunicaciones en función de la dificultad o facilidad de su coexistencia, con orden de prelación o prioridad entre ellos si deben compartir las frecuencias.

125. NECESIDAD DE LA GESTION Y/O REGULACION DEL ESPECTRO RADIOELECTRICO

a. El espectro radioelectrico es un recurso natural que está disponible y al alcance de todos. Puede ser calificado como un recurso de carácter limitado y en determinadas circunstancias (bandas y lugares geográficos) puede calificarse de escaso. Es limitado porque tiene sus fronteras definidas nítidamente, ya que más allá de la porción de 9Khz a 3000 Ghz, no se utiliza para propósitos de comunicaciones.
b. Si bien es cierto que actualmente solo es técnicamente explotable aproximadamente un 2% de dicho recurso (los primeros 60 Ghz) y están técnicamente disponibles y atribuidas internacionalmente los primeros 300 Ghz (un 10% del total), no es menos cierto que en determinadas partes del espectro y en ciertas áreas geográficas más o menos extensas (primeros 1000 Mhz y en áreas fuertemente pobladas e industrializadas) el espectro radioeléctrico se encuentra al borde de la saturación.
c. Por otra parte, el hecho de la masificación del uso del espectro radioeléctrico, así como la aparición de múltiples tipos de servicios de comunicaciones inhalámbricas, ha ocasionado la aparición de una multitud de operadoras de servicios de telecomunicaciones comerciales y redes privadas de nivel global que demandan medios de trasmisión seguros y confiables para el establecimiento de los servicios que ofrecen y/o requieren; y todo ello en el menor tiempo posible. Esta relativa escasez del dominio público radioeléctrico y el incremento de su uso como consecuencia de los avances tecnológicos, han hecho necesario e imprescindible la regulación, la gestión y/o administración internacional del uso del espectro radioeléctrico, para garantizar su aprovechamiento racional y económico del mismo.

126. REGULACION, GESTION, ADMINISTRACION Y/O CONTROL DEL ESPECTRO RADIOELECTRICO

a. Todas las naciones del mundo comparten el espectro electromagnético y se reservan sus derechos para su uso ilimitado. Sin embargo, para fines de cooperación internacional de telecomunicaciones y para apoyar al comercio, al transporte, a las comunicaciones así como la protección mutua contra la interferencia; las naciones han acordado un convenio internacional de telecomunicaciones que sirva como instrumento básico de cooperación. Este instrumento es conocido como la UNION INTERNACIONAL DE TELECOMUNICACIONES (UIT) que cuenta a su vez con una serie de conferencias, organizaciones, comités, acuerdos, manuales y otros innumerables mecanismos que posibilitarán la regulación, la gestión, la planificación, la administración y/o el control del espectro radioeléctrico.
b. En cada país deberá existir una Administradora responsable de la regulación, gestión, administración y/o control nacional del espectro radioeléctrico (ERE) dentro de su territorio. En el Perú lo es la DIRECCION GENERAL DE TELECOMUNICACIONES (DGT) del Ministerio de Transporte, Comunicaciones, Vivienda y Construcción (MTCV y C). En el Sector Defensa, el CCFA es el responsable de regular, administrar, controlar y distribuir las frecuencias para todos los institutos armados y Policía Nacional, en coordinación con la DGT.

127. BREVE HISTORIA Y RESPONSABILIDADES DE LA UIT PARA LAS RADIOCOMUNICACIONES

a. Como las ondas radioeléctricas atraviesan las fronteras nacionales y muchos sistemas de radiocomunicaciones funcionan a escala mundial para apoyar a servicios de comunicaciones, de comercio y de viajes internacionales; la comunidad internacional ha venido desarrollando una serie de mecanismos de cooperación a medida que iba evolucionando la tecnología radioeléctrica. El primer hito de cooperación internacional en el campo de las telecomunicaciones se remonta a la creación de la UNION TELEGRAFICA INTERNACIONAL en París, en 1865. Sin embargo la cooperación internacional en materia de radiocomunicaciones se inicio en 1903 con la CONFERENCIA PRELIMINAR SOBRE RADIOTELEGRAFIA SIN HILOS, que logra consolidarse en 1906 en Berlín con la PRIMERA CONFERENCIA RADIOTELEGRAFICA.

b. En esta primera Conferencia Radiotelegráfica se acuerda por primera vez el primer cuadro de atribución de bandas de frecuencia entre 500 y 1000 Khz para la correspondencia pública en el servicio marítimo, una banda de frecuencias (por debajo de 188 Khz) para comunicaciones de larga distancia para las estaciones costeras y otra banda (188-500 Khz) para estaciones militares y navales no abiertas a la correspondencia pública.

c. Con el objeto de facilitar esta cooperación internacional, se desarrollaron estructuras y procedimientos organizativos a través de conferencias cada 3 a 5 años. En Washington durante 1927, una conferencia estableció el COMITÉ CONSULTIVO INTERNACIONAL DE RADIOCOMUNICACIONES (CCIR) que estudiaría los problemas técnicos de las radiocomunicaciones. Finalmente en 1932, los países participantes en la Conferencia de Madrid, decidieran crear una organización única que hoy se le conoce como la UIT, dirigida por un solo Convenio Internacional de Telecomunicaciones complementado por el Reglamente Telegráfico, el Reglamento Telefónico y el Reglamento de Radiocomunicaciones. Entre los resultados de la conferencia de Madrid que tuvieron repercusión en las radiocomunicaciones cabe citar las siguientes:
   (1) La primera división del mundo en dos regiones, a efectos de atribución de bandas de frecuencia (Europa y los demás países).
   (2) El establecimiento de dos cuadros técnicos (uno sobre tolerancias de frecuencias y otro sobre anchuras de bandas aceptables)
   (3) El establecimiento de normas para el registro de nuevas estaciones.

d. En la Conferencia de Atlantic City de 1947, se crea la JUNTA INTERNACIONAL DE REGISTRO DE FRECUENCIAS (IFRB: International Frecuency Registration Board) con la finalidad de:
   (1) Realizar una inscripción ordenada de las asignaciones de frecuencias efectuadas a las estaciones por los distintos países.
   (2) Efectuar una inscripción ordenada de las posiciones orbitales asignadas por los países a los satélites geoestacionarios.
   (3) Asesorar a los países sobre la utilización eficaz del espectro y la órbita de los satélites geoestacionarios
   (4) Seguir los procedimientos establecidos por el Reglamento de Radiocomunicaciones o por las conferencias Administrativas.

e. Desde su creación la UIT utiliza una cierta variedad de estructuras y reuniones asociadas para llevar a cabo sus actividades. Las CONFERENCIAS ADMINISTRATIVAS DE RADIOCOMUNICACION

MUNDIAL (WARC: World Administrative Radio Conference) examinan y modifican de forma total o parcial el Reglamento de Radiocomunicaciones que contiene disposiciones técnicas y de procedimiento relativas a los diversos servicios de radiocomunicaciones. Por otro lado las CONFERENCIAS DE PLENIPOTENCIARIOS que se celebran cada cuatro años, considera la política general de actuación de la UIT para conseguir sus objetivos; ellos revisan el Convenio, establecen el presupuesto y eligen a los miembros del Consejo y a otros funcionarios de la UIT.

f. En 1992, la UIT revisó su estructura y estableció tres sectores: Sector de Desarrollo de las Telecomunicaciones, Sector de Normalización de las Telecomunicaciones y Sector de Radiocomunicaciones. La mayoría de las responsabilidades asumidas anteriormente por las secretarías especiales del CCIR y la IFRB fueron transferidas respectivamente a la OFICINA DE RADIOCOMUNICACIONES (BR: Board Radio) y a la JUNTA DEL REGLAMENTO DE RADIOCOMUNICACIONES (RRB: Regulation Radio Board) que no tiene carácter permanente. (Ver Figura 03 Estructura de la UIT).

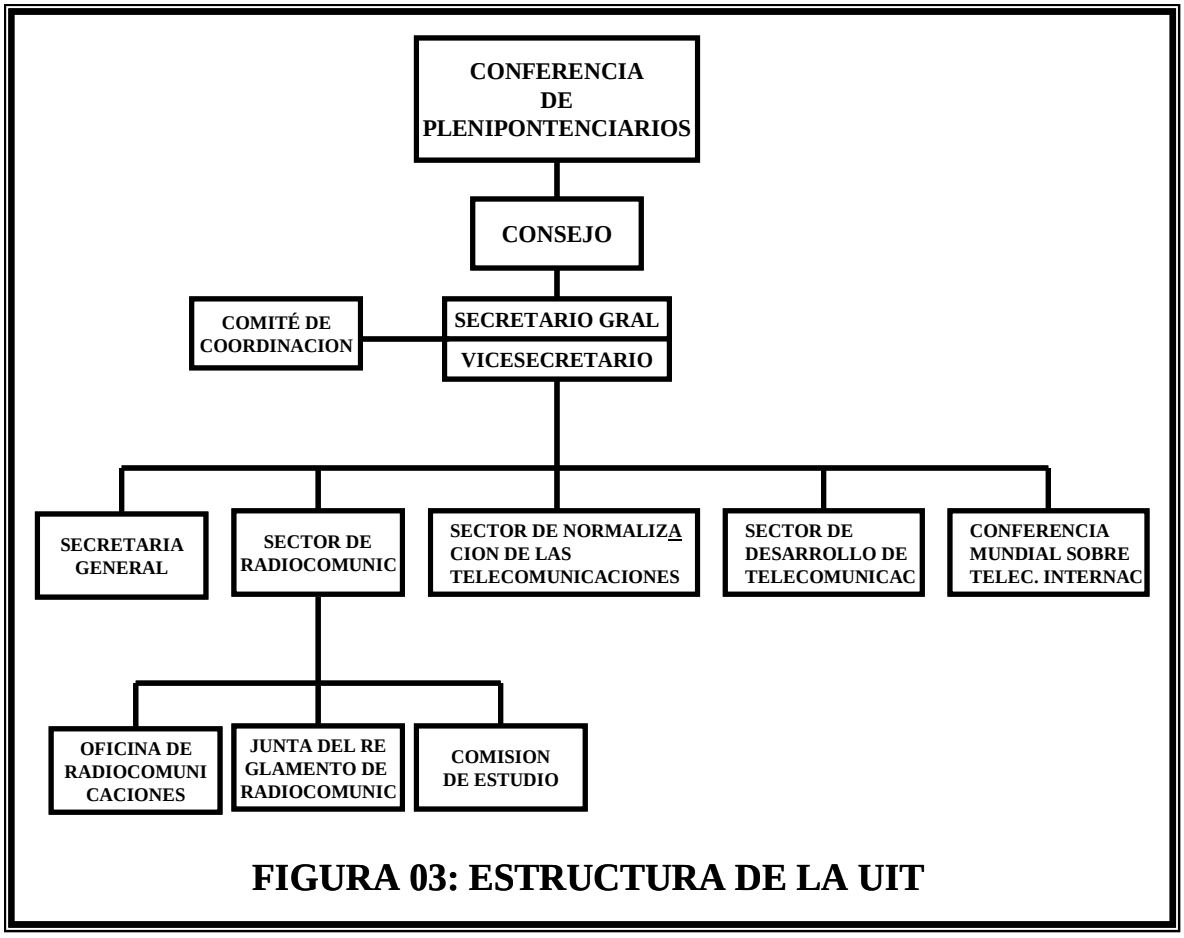


FIGURA 03: ESTRUCTURA DE LA UIT

g. Las tareas de la Oficina de Radiocomunicaciones de la UIT, incluyen:
   (1) El procedimiento de las notificaciones de asignación de frecuencias incluida la información sobre posiciones orbitales de satélites geoestacionarios, recibidas de las administradoras nacionales para su inscripción en el Registro Internacional de Frecuencias.

(2) El procesamiento de la información recibida en aplicación de los procedimientos del Reglamento de Radiocomunicaciones.
(3) El procesamiento y coordinación de los horarios estacionales de radiodifusión en ondas decamétricas.
(4) La compilación periódica de listas de frecuencias que reflejen los datos inscritos en el Registro Internacional de Frecuencias.
(5) El examen y actualización del Registro Internacional de Frecuencias.
(6) El estudio metódico, a largo plazo, de la utilización del espectro con el objeto de asegurar una máxima eficacia.
(7) La investigación de los casos de interferencia perjudicial.
(8) La prestación de ayuda a las administradoras en el campo de la utilización del espectro radioeléctrico y la capacitación del personal.
(9) La recopilación de los resultados de las observaciones de comprobación técnica de las emisiones.
(10) El desarrollo de las reglas de procedimiento.
(11) La prestación de apoyo técnico y administrativo a las Conferencias de Radiocomunicaciones, a las Asambleas de Radiocomunicaciones y a las actividades de las Comisiones de Estudio.
(12) La publicación y el entrenamiento sobre el Reglamento de Radiocomunicaciones; sobre los procedimientos administrativos y estándares; y sobre las Recomendaciones de la UIT-R (anteriormente conocida como CCIR) y de manuales sobre características de los sistemas de radiocomunicaciones y utilización del espectro.

h. Las actividades de la Junta del Reglamento de Radiocomunicaciones actualmente incluyen un rol de arbitraje y revisión formal, que asegure coherencia en la aplicación de decisiones de la conferencia y la resolución de asuntos extraordinarios; tales como:
(1) La aprobación de las reglas de procedimientos, que incluyen criterios técnicos, de acuerdo con el Reglamento de Radiocomunicaciones y con cualquier decisión que puedan tomar las Conferencias de Radiocomunicaciones competentes.
(2) La consideración de cualquier otro asunto que no pueda resolverse mediante la aplicación de las reglas de procedimiento.
(3) La regulación de tareas adicionales relativos a la asignación y utilización de las frecuencias.
(4) El Reglamento de Radiocomunicaciones (RR) constituye el acuerdo internacional fundamental relativo a reglas y procedimientos para el funcionamiento de los equipos radioeléctricos y la resolución de problemas de interferencia. **El Cuadro de atribución de bandas de frecuencias, contenido en el artículo 8 del RR, sirve de base para la asignación nacional de frecuencias.**

i. Las Comisiones de Estudio de Radiocomunicaciones, estudian problemas y formulan Recomendaciones sobre:
(1) El uso del espectro de radiofrecuencias en radiocomunicaciones terrestre y espacial (y de satélites de órbita geoestacionaria)
(2) Las características y el desempeño de sistemas radioeléctricos
(3) La operación de estaciones radioeléctricas
(4) Los aspectos de peligro y seguridad en radiocomunicaciones.

j. Con el fin de ayudar a las Administradoras Nacionales en el desarrollo y la aplicación de sistemas eficaces de gestión del espectro, la UIT desarrolló el

MANUAL SOBRE GESTION NACIONAL DEL ESPECTRO, que abarca los puntos siguientes:

(1) Principios fundamentales de la gestión del espectro.
(2) Planificación del espectro
(3) Prácticas de ingeniería del espectro
(4) Autorización de frecuencias
(5) Utilización del espectro (incluyendo su eficacia)
(6) Control del espectro (inspección y control)
(7) Automatización de la gestión del espectro.

SECCION II. ADMINISTRACION NACIONAL DEL ESPECTRO RADIOELECTRICO

128. MARCO LEGAL BASICO DE LAS TELECOMUNICACIONES EN EL PERU

a. Con Decreto Supremo N° 013-93-TCC se aprobó el Texto Unico Ordenado de la "Ley de Telecomunicaciones", que declaró de "necesidad pública el desarrollo de las telecomunicaciones como instrumento de pacificación y de afianzamiento de la conciencia nacional .....". Posteriormente con Decreto Supremo N° 06-94-TCC se aprobó el Reglamento General de la Ley de Telecomunicaciones, que en su Artículo 1° establece: ".... las disposiciones generales para la prestación de los servicios de telecomunicaciones, la administración del espectro radioeléctrico, la normalización y homologación de equipos y aparatos de telecomunicaciones y la regulación del mercado de servicios .....".
b. La Ley y el Reglamento Gral de la Ley de Telecomunicaciones establece que los Servicios de Telecomunicaciones, dentro del concepto de Red Digital Integrada de Servicios y Sistemas, se clasifican en:
   (1) Servicios Portadores.
   (2) Teleservicios o Servicios Finales
   (3) Servicios de Difusión
   (4) Servicios de Valor Añadido o Agregado
c. Igualmente el Art 16° del Reglamento señala "En los estados de excepción contemplados en la Constitución y declarados conforme a Ley, todos los operadores de servicios portadores y teleservicios deben otorgar prioridad a la trasmisión de voz y data necesaria para los medios de comunicación de los Sistemas de Defensa Nacional y Defensa Civil. En caso de guerra exterior declarada conforme a ley, el Consejo de Defensa Nacional a través del CFFAA, podrá asumir el control directo de los servicios de telecomunicaciones, así como dictar disposiciones de tipo operativo ....".
d. El título VIII Del Espectro Radioeléctrico, título IX De los Derechos de Tasas y Canon y Título X Normalización y homologación del Reglamento de la Ley de telecomunicaciones establece los aspectos fundamentales siguientes:
   (1) El espectro radioeléctrico constituye un recurso natural limitado que forma parte del patrimonio de la nación. Corresponde al MT y C la administración, la asignación y el control del espectro (Art 183º)
   (2) El Plan Nacional de Asignación de Frecuencias, es el documento técnico normativo que contiene los cuadros de atribución de frecuencia a los servicios de telecomunicaciones, así como las normas técnicas generales para utilización del espectro (Art. 184º).

(3) **El MTCV y C atribuirá las bandas de frecuencias para la operación de los servicios de telecomunicaciones de las Fuerzas Armadas y PNP previa coordinación con el Comando Conjunto de las Fuerzas Armadas, las mismas que estarán contenidas en el Plan Nacional de Atribución de Frecuencias (Art. 184º).**

(4) El Plan Nacional de Atribución de Frecuencias, contendrá los cuadros de atribución para la utilización del espectro radioeléctrico sobre la base de prioridades nacionales. Dicho Plan indicará la clase y categoría de servicios de telecomunicaciones para cada una de las bandas de frecuencias, **de conformidad con el Reglamento de Radiocomunicación, anexo al Convenio de la UIT, debiendo contemplar las necesidades de los Sistemas de Defensa y Seguridad Nacional (Art. 187º).**

(5) La DGT llevará un Registro Nacional de Frecuencias en el que se inscribirán las asignaciones que haya efectuado. El MTC establecerá el procedimiento y forma de acceso del público a la información de dicho registro, teniendo en cuenta su grado de confidencialidad y la Seguridad nacional (Art. 191º).

(6) Está prohibido el uso de estaciones radioeléctricas para finalidad diferente a la autorizada, excepto en apoyo de los sistemas de defensa nacional o civil y durante los estados de excepción (Art. 195º).

(7) Para el control del espectro radioeléctrico el MTC podrá efectuar la comprobación técnica de las emisiones radioeléctricas, identificar y localizar las interferencias perjudiciales, detectar a las personas que presten servicios de telecomunicaciones en condiciones técnicas distintas a las establecidas; todas estas acciones podrá hacerlas a través de las "Entidades Inspectoras" (Art 201º).

(8) No están afectos al pago del canon anual por el uso del espectro radioeléctrico las estaciones operadas por entidades del Gobierno Central (Art. 212º)

(9) El objetivo de la homologación de equipos y aparatos de telecomunicaciones es asegurar el adecuado cumplimiento de las especificaciones técnicas a que éstos deben sujetarse para prevenir daños a las redes que se conecten, evitar interferencias a otros servicios de telecomunicaciones y garantizar la seguridad del usuario (Art. 220º).

(10) El MTC podrá encargar a terceros la realización de las pruebas necesarias para la normalización y homologación de equipos y aparatos de acuerdo a especificaciones técnicas de la UIT. La personal o personas encargadas de tales pruebas serán denominadas "Entidades Verificadoras" (Art. 223º).

129. PLAN NACIONAL DE ATRIBUCIÓN DE FRECUENCIAS

a. Con Resolución Ministerial N° 250-97-MTC/15.19, publicada en el diario Oficial El Peruano el 20 de Junio de 1997, se aprobó el PLAN NACIONAL DE ATRIBUCION DE FRECUENCIAS con el siguiente tabla de contenido:

(1) Capítulo I. Terminología
Artículo 1
Sección I, Términos Generales
Sección II, Términos Específicos relativos a la gestión de

frecuencias
Sección III, Servicios radioeléctricos
Sección IV, Estaciones y Servicios radioeléctricos
Sección V, Términos referentes a la explotación
Sección VI, Características de las emisiones y equipos
Sección VII, Compartición de frecuencias
Sección VIII, Términos técnicos relativos al espacio
Artículo 2, Nomenclatura de las bandas de frecuencia y de las Longitudes de ondas empleada en las radiocomunicaciones.
Artículo 3, Denominaciones de las Emisiones
Sección I, Anchura de banca necesaria
Sección II, Clases de emisiones.

(2) Capítulo II. Atribución de bandas de frecuencia
Artículo 4, Descripción de las regiones y zonas del mundo y cuadro de atribución de bandas de frecuencias.
Sección I, Regiones y zonas del mundo
Sección II, Categorías, servicios y las atribuciones.
Sección III, Disposiciones del cuadro de atribución de las bandas de frecuencias.
Sección IV, Cuadro de atribución de bandas de frecuencias
Sección V, Notas y observaciones del cuadro de atribución de bandas de frecuencia.

b. Los principales términos y definiciones de interés son:

(1) Radiodeterminación.- Es la determinación de la posición, velocidad u otras características de un objeto u obtención de información relativa a estos parámetros, mediante las propiedades de propagación de las ondas radioeléctricas.

(2) Radiolocalización.- Es la radiodeterminación utilizada para fines distintos de radionavegación.

(3) Radiogoniometría.- Es la radiodeterminación que utiliza la recepción de ondas radioeléctricas para determinar la dirección de una estación o de un objeto.

(4) Tiempo Universal Coordinado (UTC).- Escala de tiempo basada en el segundo (SI), definida y recomendada por la UIT-R (antes CCIR) y mantenida por la Oficina Internacional de la hora (BIH). El UTC es equivalente a la hora solar media en el meridiano origen (0º de longitud), anteriormente expresada en GMT.

(5) Atribución de una frecuencia o de un canal radioeléctrico.- Es la inscripción en el Cuadro de atribución de bandas de frecuencias, de una banda de frecuencias determinada, para que sea utilizada por uno o varios servicios de radiocomunicación terrenal o espacial.

(6) Adjudicación de una frecuencia o de un canal radioeléctrico.- Es la inscripción de un canal determinado en un plan, adoptado por una conferencia competente, para ser utilizado por una o varias administraciones para un servicio de radiocomunicación terrenal o espacial en uno o varios países o zonas geográficas determinadas y según condiciones especificadas.

(7) Asignación de un frecuencia o de un canal radioeléctrico.- Es la autorización que da una administración para que una estación

radioeléctrica utilice una frecuencia o un canal radioeléctrico determinado en condiciones especificadas.

(8) Banda de frecuencias asignada.- Es la banda de frecuencias en el interior de la cual se autoriza la emisión de una estación determinada; la anchura de esta banda es igual a la anchura de banda necesaria más el doble del valor absoluto de la tolerancia de frecuencia.

(9) Frecuencia asignada.- Es el centro de la banda de frecuencias asignadas a una estación.

(10) Frecuencias característica.- Es la frecuencia que puede identificarse y medirse fácilmente en una emisión determinada (por ejemplo una frecuencia portadora).

(11) Frecuencia de referencia.- Es la frecuencia que ocupa una posición fija y bien determinada con relación a la frecuencia asignada. La desviación de esta frecuencia con relación a la frecuencia asignada es, en magnitud y signo la misma que la de la frecuencia característica con relación al centro de la banda de frecuencias ocupada por la emisión.

(12) Tolerancia de frecuencia.- Es la desviación máxima admisible entre frecuencia asignada y la situada en el centro de la banda de frecuencias ocupada por una emisión, o entre la frecuencia de referencia y la frecuencia característica de una emisión (Se expresa en hertzios o en millonésimas).

(13) Anchura de banda necesaria.- Para una clase de emisión dada, anchura de la banda de frecuencias es la estrictamente suficiente para asegurar la trasmisión de la información a la velocidad y con la calidad requeridas en condiciones especificadas.

(14) Radiación radioeléctrica.- Es el flujo saliente de energía de una fuente cualquiera en forma de ondas radioeléctricas, o esta misma energía.

(15) Emisión.- Es la radiación producida, o producción de radiación, por una estación trasmisora radioeléctrica.

(16) Clase de emisión.- Conjunto de características de una emisión, a saber tipo de modulación de la portadora.

(17) Potencia.- Siempre que se haga referencia a la potencia de un trasmisor radioeléctrico, etc., ésta se expresará, según la clase de emisión, en una de las formas siguientes, utilizando para ello los símbolos convencionales que se indican:

- potencia en la cresta de envolvente (PX ó pX)
- potencia media (PY ó pY)
- potencia de la portadora (PZ ó pZ)

En las fórmulas, el símbolo “p” indica la potencia en vatios y el símbolo “P” la potencia en decibeles relativa a un nivel de referencia.

(18) Zona de Cobertura.- Es la zona asociada a una estación trasmisora para un servicio dado y una frecuencia específica, en el interior de la cual y en condiciones técnicas determinadas, puede establecerse una radiocomunicación con otra u otras estaciones receptoras.

(19) Zona de Servicio.- Es la zona asociada a una estación para un servicio dado y una frecuencia específica, en el interior de la cual y en condiciones técnicas determinadas, puede establecerse una radiocomunicación con una o varias estaciones ya existente o previstas, y en la que debe respetarse la protección fijada por un Plan o por una disposición técnica emanada de la DGT.

130. NOMENCLATURA DE LAS BANDAS DE FRECUENCIAS Y DE LAS LONGITUDES DE ONDA EMPLEADAS EN LAS RADIOCOMUNICACIONES

a. A un conjunto particular de frecuencias de radio se le llama banda de frecuencias. Todas las bandas de frecuencias están contenidas dentro del espectro radioeléctrico, y éste es parte del espectro electromagnético.

b. Las bandas de radiofrecuencia son comúnmente designadas y referidas con un sistema de abreviaturas o símbolos acordados internacionalmente dentro de la UIT y acogidos en el Plan Nacional de Atribución de Frecuencias (Art. 2), y son:

N° DE LA BANDA	FRECUENCIA	SIMBOLO	SIGNIFICADO	SUBDIVISION METRICA CORRESPONDIENTE
2	Menos de 300	ELF	Extremada baja frecuencia	-
3	300 – 3000 Hz	ILF	Intermedia baja frecuencia	-
4	3 - 30 Khz	VLF	Muy baja frecuencia	Miriametricas
5	30 - 300 Khz	LF	Baja frecuencia	Kilométricas
6	300 - 3000 Khz	MF	Frecuencia media	Hectométricas
7	3 - 30 Mhz	HF	Alta frecuencia	Decamétricas
8	30 - 300 Mhz	VHF	Muy alta frecuencia	Métricas
9	300 - 3000 Mhz	UHF	Ultra alta frecuencia	Decimétricas
10	3 - 30 Ghz	SHF	Super alta frecuencia	Centimétricas
11	30 - 300 Ghz	EHF	Extremada alta frecuencia	Milimétricas
12	300 - 3000Ghz	-	-	Decimilimétricas

c. La “banda N” (N = número de la banda) se extiende de 0.3×10^n Hz a 3×10^n Hz. Normalmente las bandas de ELF y VLF son para frecuencias empleadas en equipos de sonar. El espectro radioeléctrico va desde los 3 Khz hasta los 3×10^5 Mhz (EHF ó 300 Ghz).

d. Después del espectro radioeléctrico el espectro electromagnético tiene las frecuencias y usos siguientes:
   (1) De 3×10^5 Mhz a 3×10^8 Mhz para Rayos Infrarojos
   (2) De 3×10^7 Mhz a 3×10^8 Mhz para detección de calor y guiado de misiles (radar)
   (3) De 3×10^8 Mhz a 3×10^9 Mhz para luz visible
   (4) De 3×10^9 Mhz a 3×10^{13} Mhz para rayos ultravioleta y rayos “x” (medicina)
   (5) De 3×10^{12} Mhz a 3×10^{15} Mhz para rayos gamma
   (6) De 3×10^{14} Mhz hacia delante para los rayos cósmicos y para la detección de radioactividad.

e. En la figura 4, Espectro radioeléctrico, uso y características de propagación; se muestran las frecuencias y principales empleos con sus características de propagación.

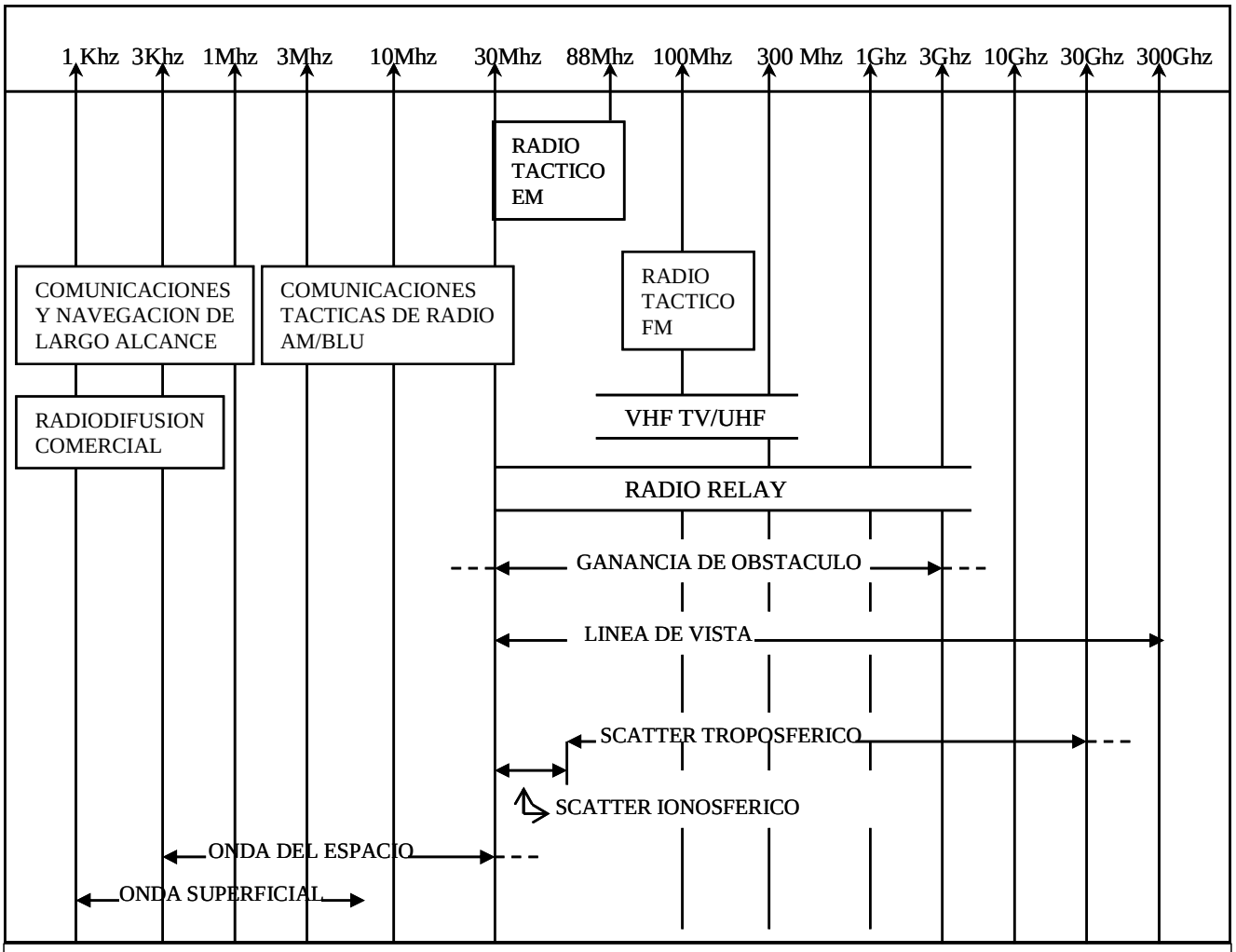


FIGURA 04: ESPECTRO RADIOELECTRICO, USO Y CARACTERISTICAS

131. DENOMINACIÓN DE LAS EMISIONES

a. Las emisiones se denominarán conforme a:
   (1) Anchura de la banda necesaria
   (2) Clase de emisiones

b. Anchura de la banda necesaria
   (1) Se expresa mediante 3 cifras y una letra. La letra ocupará la posición de la coma decimal, representando la unidad de la anchura de banda. Esta expresión no podrá comenzar por cero ni por K, M, o G.
   (2) La anchura de banda necesaria de expresa:
      (a) En Hz (letra H) para frecuencias entre 0,001 y 999
      (b) En Khz (letra K) para frecuencias entre 1,00 y 999 Khz
      (c) En MHz (letra M) para frecuencias entre 1,00 y 999 Mhz
      (d) En Ghz (letra G) para frecuencias entre 1,00 y 999 Ghz
   (3) Ejemplos:

(a) 0,002 Hz = H002	(f) 6 Khz = 6K00	(k) 1,25 Mhz = 1M25
(b) 0,1 Hz = H100	(g)12,5 Khz = 12K5	(l) 2 Mhz = 2M00
(c) 25,3 Hz = 25H3	(h)180,4Khz = 180K	(m) 10 Mhz = 10M0
(d) 400 Hz = 400H	(i) 180,5Khz = 181K	(n) 202 Mhz = 202M
(e) 2,4 Khz = 2K40	(j) 180,7Khz = 181K	(ñ) 5.65 Ghz = 5G65

c. Clases de emisiones

(1) La emisiones se clasifican y simbolizan de acuerdo con:
   (a) Sus características esenciales
   (b) Sus características adicionales

(2) Las características esenciales son:
   (a) Primer símbolo.- Indica el tipo de modulación de la portadora principal (ver cuadro 1)
   (b) Segundo símbolo.- Indica la naturaleza de la señal (o Telemática) que modula (n) la portadora principal (ver cuadro 2).
   (c) Tercer símbolo.- Indica el tipo de información que se va a trasmitir (ver cuadro 3).

(3) Las características adicionales son:
   (a) Cuarto símbolo.- Indica los detalles de la señal (es). Su uso será opcional cuando sea aplicable (ver cuadro 4).
   (b) Quinto símbolo.- Indica la naturaleza del multiplaje. Su uso también será opcional cuando sea aplicable (ver cuadro 5).

(4) La modulación puede no tomarse en cuenta si se utiliza sólo durante cortos periodos y de manera incidental (por ejemplo en caso tales como identificación o llamada) siempre que no aumente la anchura de banda necesaria indicada.

CUADRO 01 : TIPO DE MODULACIÓN DE LA PORTADORA PRINCIPAL

SIMBOLO	TIPO DE EMISIÓN
N	NO MODULADA Emisión de una portadora no modulada
	AMPLITUD MODULADA (AM) Emisión en la cual la portadora principal está modulada en amplitud (incluidos los casos en en que las subportadoras tengan modulación angular)
A	Doble banda lateral
B	Bandas laterales independientes
C	Banda lateral residual
H	Banda lateral única (BLU), portadora completa
J	Banda lateral única (BLU), portadora suprimida
R	Banda lateral única (BLU), portadora reducida o de nivel variable
	MODULACIÓN ANGULAR Emisión en que la portadora principal tiene modulación angular
F	Frecuencia modulada (FM)
G	Modulación en fase
D	AMPLITUD MODULADA Y MODULACIÓN ANGULAR Emisión en la cual la portadora principal puede tener modulación de amplitud y modulación angular, bien simultáneamente o según una secuencia pre-establecida.
	PULSO Emisión de impulsos: emisiones donde la portadora principal está directamente modulada por una señal que ha sido codificada en forma cuantificada (por ejemplo, la modulación por pulsos codificados) deberán designarse como en amplitud modulada o modulación angular.
P	Secuencia de pulsos no-modulados

	Secuencia de Pulsos:
K	Modulados en amplitud
L	Modulados en anchura/duración
M	Modulados en posición/fase
Q	Cuando la portadora tiene modulación angular durante el periodo del pulso
V	Combinación de las técnicas precedentes o que se producen por otros medios
	COMBINACIÓN
W	Casos no cubiertos arriba, en los que una emisión consiste de la portadora principal modulada, bien simultáneamente, según una secuencia previamente establecida, o según una combinación de dos o más de los modos siguientes: AM, modulación angular o por pulsos (nQAM, nTCM u otros)
X	Casos no previstos

CUADRO 02 : NATURALEZA DE LA SEÑAL (ES) QUE MODULA (N(LA PRTADORA PRINCIPAL

SIMBOLO	TIPO DE EMISIÓN
0	Ausencia de señal moduladora
1	Un solo canal de información cuantificada o digital, sin utilizar una subportadora (se excluye el multiplaje por división de tiempo)
2	Un solo canal con información cuantificada o digital, utilizando una subportadora
3	Un solo canal con información analógica (voz)
7	Dos o más canales con información cuantificada o digital
8	Dos o más canales con información analógica
9	Sistema compuesto con uno o más canales con información cuantificada o digital, junto con uno o más canales con información analógica.
X	Casos no previstos

CUADRO 03 : TIPO DE INFORMACIÓN A TRASMITIRSE

SIMBOLO	TIPO DE EMISIÓN
N	Ausencia de información trasmitida
A	Telegrafía (para recepción acústica)
B	Telegrafía (para recepción automática)
C	Facsimil
D	Trasmisión de datos, Telemetría, Telecomando
E	Telefonía (incluída la radiodifusión sonora)
F	Televisión (video)
W	Combinación de los procedimientos anteriores
X	Casos no previstos

CUADRO 04: DETALLES DE LA SEÑAL (ES)	
SIMBOLO	TIPO DE EMISIÓN
A	Código de dos estados con elementos que diferencien en número y/o duración
B	Código de dos estados con elementos idénticos en número y duración, sin corrección de errores.
C	Código de dos estados con elementos idénticos en número y duración, con corrección de errores.
D	Código de cuatro estados, cada uno de los cuales representa un elemento de señal (de uno o o varios bitios)
E	Código de múltiples estados, cada uno de los cuales representan un elementos de señal (de uno o de varios bitios)
F	Código de múltiples estados en el cual cada estado o combinación de estados representa un carácter.
G	Sonido de calidad de radiodifusión (monofónico)
H	Sonido de calidad de radiodifusión (estereofónico o cuadrifónico)
J	Sonido de calidad comercial (excluidas las categorías definidas por los símbolos K y L que siguen)
K	Sonido de calidad comercial con utilización de inversión de frecuencia o división de banda.
L	Sonido de calidad comercial con Telemática separadas moduladas en frecuencias para controlar el nivel de la señal modulada.
M	Señal monocromática (blanco y negro)
N	Señal de color
W	Combinación de los casos anteriores
X	Casos no previstos

CUADRO 05 : NATURALEZA DEL MULTIPLAJE	
SIMBOLO	TIPO DE EMISIÓN
N	Ausencia del multiplaje
C	Multiplaje con división de códigos (incluye técnicas de expresión de ancho de banda)
F	Multiplaje por división de frecuencias
T	Multiplaje por división de tiempo
W	Combinación de multiplaje por división de frecuencias y división de tiempo.
X	Otros tipos de multiplaje.

d. La denominación de las emisiones deberían emplearse de acuerdo a los reglamentos siguientes: "Entrar primero la anchura de banda necesaria y luego entrar el designador de emisión básica de los símbolos de características esenciales, y si se desea, los otros dos opcionales de características adicionales". ejm:

DENOMINACIÓN		SIGNIFICADO
ANCHURA DE BANDA	CLASE DE EMISIÓN	
3K 00	J3E	3Khz de ancho de banda, BLU portadora suprimida, canal único de voz para telefonía.
30K 0	F3E	30 Khz de ancho de banda, FM, canal único de voz para telefonía.

132. PRINCIPALES FRECUENCIAS DE PROPOSITO ESPECIAL

a. Los acuerdos internacionales y nacionales, así como el propio Plan Nacional de Atribución de frecuencias, han designado frecuencias de propósito especial empleadas dentro de cualesquiera de las 3 regiones (el Perú pertenece a la Región 2), sólo dentro de la Región 2 o dentro del territorio nacional.

b. Estas frecuencias sólo podrán emplearse para las aplicaciones que han sido acordadas, normalmente para desastres marítimos, búsqueda y rescate, desastres aeronáuticos, etc.

c. Estas frecuencias y sus usos son:

(1) **500 Khz**.- Es la frecuencia internacional de socorro y llamada de radiotelegrafía morse.

(2) **2,187,5Khz; 4207,5 Khz; 6321 Khz; 8414,5 Khz y 16804,5 Khz** .- Son frecuencias internacionales de socorro para la llamada selecta digital.

(3) **2174,5 Khz; 4177,5 Khz; 6268 Khz; 8376,5 Khz; 12520 Khz y 16695 Khz**.- Son frecuencias internacionales de socorro para telegrafía de impresión directa de banda angosta.

(4) **3,5 Mhz; 7 Mhz; 14 Mhz; 18,068 Mhz; 21 Mhz y 144 Mhz**.- Son frecuencias que podrán ser utilizados por el MTCVyC, en casos de catástrofes naturales dentro de las bandas atribuidas al servicio de aficionados fijo/móvil (3.5 a 3.75/7 a 7.3/10.1 10.15/14 a 14.25 (sat)/18.068 a 18.168 (sat)/21 a 21.45 (sat)/24.89 a 24.99 (sat) y 144 a 146 (sat)).

(5) El uso de la banda **4000-4063 Khz**, por el servicio móvil marítimo, está limitado a las estaciones de barco que funcionan en radiotelefonía.

(6) **4209,5 Khz** es la frecuencia que se utilizará exclusivamente para la trasmisión por las estaciones costeras de aviso a los navegantes, boletines meteorológicas con destino a los barcos mediante técnicos de impresión directa de banda estrecha.

(7) **4210 Khz; 6314 Khz; 8416,5 Khz; 12579 Khz; 16806,5 Khz; 19680,5 Khz y 26100,5 Khz**.- Son las frecuencias internacionales de trasmisión de información relativa a la seguridad marítima (MSI)

(8) Las bandas de frecuencia central **13560 Khz; 27120 Khz; 40,68 Mhz; 915 Mhz; 2450 Mhz; 5800 Mhz y 24,125 Ghz** están destinadas para aplicaciones industriales, científicas y médicas (ICM). Los servicios de radiocomunicación que funcionen en estas bandas deben aceptar la interferencia perjudicial resultante de estas aplicaciones y en ningún caso podrán causar interferencias a aplicaciones ICM. Las bandas 2400 - 2483,5 Mhz y 5725-5850 Mhz están atribuidos a titulo secundario al servicio fijo que utilice tecnología de espectro ensanchado e igualmente no están sujetos a protección y no deberán ocasionar interferencia perjudicial a los demás servicios que operan en estas bandas

(9) **Las bandas. 5900-5950 Khz; 7300-7350 Khz; 9400-9500 Khz; 11600-11650 Khz; 12050-12100 Khz; 13570-13600 Khz; 13800-13870 Khz; 15600-15800 Khz; 17480-17550 Khz; 18900-19020 Khz**; a partir del 01Abr2007 serán atribuídas al servicio de radiodifusión de BLU.

(10) Las bandas **21870-21924, 23200-23350 Khz** son utilizadas por el servicio fijo para el suministro de servicios relacionados en la seguridad de los vuelos de aeronaves.

(11) La frecuencia de 75 Mhz se asigna a las radiobalizas aeronáuticas.

(12) Las frecuencias de 54 a 72 Mhz y de 76 a 88 Mhz se asignan a la radiodifusión televisiva .
(13) La banda de 88 a 108 Mhz se empleará en radiodifusión sonora en FM y para servicios públicos de telecomunicaciones, utilizando las subportadoras.
(14) **121.5 Mhz y 123.1 Mhz** son frecuencias aeronáuticas de emergencia. Las estaciones móviles del servicio móvil marítimo podrán comunicarse en estas frecuencias para fines de socorro y seguridad, con las estaciones del servicio móvil aeronáutico.
(15) La frecuencia **156.525 Mhz** se utilizará exclusivamente para la llamada selectiva digital con fines de socorro, seguridad y llamada en el servicio móvil marítimo en ondas métricas.
(16) **156,8 Mhz** es la frecuencia internacional de socorro, seguridad y llamada del servicio móvil marítimo radiotelefónico en ondas métricas.
(17) Las frecuencias de **174 a 216 Mhz** son para radiodifusión televisiva.
(18) **243 Mhz** es la frecuencia de salvamento móvil aeronáutico
(19) **400,1 Mhz** es la frecuencia patrón y Telemática horarias por satélite.
(20) La banda 406-406,1 Mhz del servicio móvil por satélite está limitado a las estaciones de radiobalizas de localización de siniestros por satélites de poca potencia.
(21) Las frecuencias de 470 a 608 Mhz y 614 a 806 Mhz está asignada a la radiodifusión televisiva.
(22) Las bandas 806-824 Mhz y 851-869 Mhz están atribuidas a título primario al servicio troncalizado (canales múltiples de selección automática).
(23) Las bandas de 824-849 y 869-894 Mhz están atribuidos a título primario al servicio celular (telefonía móvil) y de 846,5-849 Mhz y 891,5-894 Mhz para fuera de Lima (banda "B") para comunicaciones rurales.
(24) La banda de 960-1215 Mhz se reserva en todo el mundo para el uso y el desarrollo de equipos electrónicos de ayudas a la navegación aérea instalados a bordo de aeronaves y de instalaciones con base de tierra directamente asociados.
(25) El empleo de las bandas de 1300-1350 Mhz, 2400-2900 Mhz y 9000-9200 Mhz por el servicio de radionavegación aeronáutica está limitado a los radares terrestres y a los respondedores aeroportados asociados que omitan sólo en frecuencias de estas bandas.
(26) La banda de frecuencias entre 1850-1990 Mhz está destinada a los servicios públicos móviles y fijos que se presten mediante sistemas de comunicaciones personales (PCS) y aplicaciones de acceso inalámbrico fijo (FWA).
(27) La banda entre 2500-2700 Mhz está destinada para el servicio público de distribución de radiodifusión por cable utilizando el sistema MMDS.

SECCIÓN III. ADMINISTRACIÓN DEL ESPECTRO DE FRECUENCIAS POR EL SECTOR DEFENSA

133. RESPONSABILIDADES DENTRO DEL MINISTERIO DE DEFENSA

a. El Secretario General del Ministerio de Defensa, a través de la secretaria de Asuntos Intersectoriales, debería ser la responsable de la coordinación de las políticas de administración del espectro radioeléctrico ante un Comité Interministerial de Asesoramiento de radio, integrado por todos los sectores que deban emplear redes y/o sistemas inalámbricos que controlen supervisen y/o administren el espectro dentro de sus respectivos ámbitos.
b. Este comité podría estar constituido por cuatro sub-comites:
   (1) De asignación de frecuencias
   (2) De planeamiento del espectro radioeléctrico
   (3) Técnica
   (4) De notificación internacional
c. Las políticas y/o directivas aprobadas al más alto nivel nacional, deberán ser puestas a conocimiento de la Secretaría de Operaciones Conjuntas, la cual deberían contar con una Oficina de Comando, control, Comunicaciones, Computadoras e Inteligencia (C^4I); la cual sería responsable ante el Secretario General del cumplimiento de dichas políticas por el sector defensa.
d. Cada instituto armado y PNP, a su vez deberá nombrar representantes o contar con Oficinas o dependencias, responsables de coordinar la administración del espectro; ya sea directamente ante el comité o a través de la 5ta DIEMFFAA, así como a través de las respectivas secretarias de cada instituto, establecer canales de coordinación para la asignación y distribución de frecuencias.
e. Lo ideal sería que se constituyera un Consejo Militar de comunicaciones y Electrónica, que fuera responsable de manera integrada, de la coordinación de los asuntos de Telecomunicaciones entre todas las Fuerzas Armadas, entre éstas y el MINDEF y con otras dependencias del sector público y privado.
f. Las funciones generales de este Consejo Militar, bajo las políticas y directivas del Secretario General de Defensa y del Jefe del EM de las fuerzas armadas; podrían ser la de guiar al sector en la preparación y coordinación técnica de las directivas, acuerdos, distribución y asignación del espectro entregado por el Comité Interministerial
g. Este Consejo podría componerse de las siguientes oficinas/puestos/responsables (existentes o por crearse):
   (1) Director de Sistemas de Comando, Control Y Comunicaciones (oficina del JEMFA).
   (2) Director de la Oficina de Comunicaciones (del MINDEF)
   (3) Director de Sistemas de Información para Comando, Control, Comunicaciones y Computadoras (del Ejército)
   (4) Director de C^4 (de la Naval)
   (5) Directos de C^4 (de la Fuerza Aérea)
   (6) Director de C^3 Táctico - conjunto
   (7) Director de representante de SIN (para asuntos de C^4)

h. Debajo de este Consejo se establecería un Panel Conjunto de Frecuencias como el principal coordinador del sector defensa para la administración del espectro radioeléctrico. este panel revisa, desarrolla, coordina e implementa las directivas del sector defensa, los estudios, informes y recomendaciones para el Consejo Militar de Comunicaciones y Electrónica. Las áreas de estudio podrán incluir administración e ingeniería de radiofrecuencia, radiopropagación y protección electrónica.

i. Asi mismo dentro del sector defensa es conveniente considerar a los Coordinadores de Frecuencia de Area, quienes serían responsables de coordinar el uso en campaña de radiofrecuencias dentro del rango de frecuencias y áreas geográficas asignadas. Normalmente el coordinador de frecuencia de area es el C-6 del TO y desde época de paz puede ser el Jefe de la Oficina de Comunicaciones de cada Región Militar.

j. En la figura 05, se muestra los canales de administración de frecuencias militares que se propone, dentro de la estructura del Ejército y su relación con el Sector Defensa.

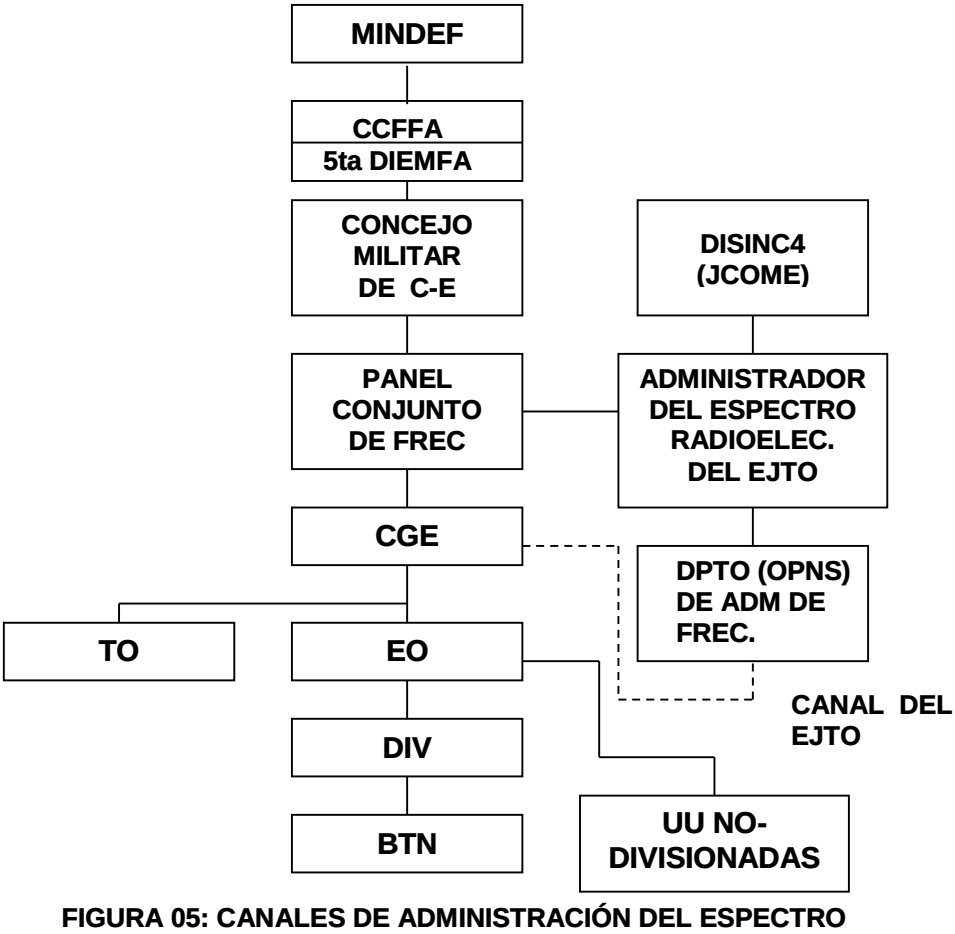


FIGURA 05: CANALES DE ADMINISTRACIÓN DEL ESPECTRO

134. RESPONSABILIDADES DENTRO DEL EJERCITO HASTA NIVEL OPERACIONAL

a. La Dirección de Sistemas de Información para el Comando, Control, Comunicaciones y Computadoras (DISIN C4), que actualmente se conoce como Jefatura de Comunicaciones y Electrónica del Ejército (JCOME),

debe contar con un Departamento de Administración de frecuencias cuyo jefe será el administrador del Espectro Radioeléctrico del Ejército.

b. A nivel TO (Región Militar), el Jefe de Oficina Regional de Comunicaciones y Electrónica, que en operaciones se le denomina C-6; será responsable del espectro radioeléctrico en su área de responsabilidad. El C-TO ejercerá el control sobre el espectro a través de este miembro de EM de coordinación y contará con una oficina de RF, cuyo jefe será el administrados del espectro.
c. El C-6 coordinará toda la interoperatividad de las comunicaciones y Telemática conjuntas, estableciendo los requerimientos totales de la fuerza y resolverá cada necesidad única de cada instituto o fuerza armada presente en el TO. Por eso, para proveer comunicaciones altamente confiables, la sección de planeamiento del C-6 debe estar ampliamente enterada de la situación táctica y estratégica sobre toda la secuencia de planeamiento. A este nivel, el administrador de las frecuencias conjuntas, obtendrá las frecuencias asignadas del administrador de las frecuencias del ejército y de los demás institutos que actúan en su área.
d. El C-6 deberá coordinar con el C-2 (Inteligencia), C-3 (Operaciones) y el Cmdte de la Unidad de Guerra Electronica; para que todas las emisiones de radio sean consideradas para el establecimiento de la LISTA DE FRECUENCIAS RESTRINGIDAS CONJUNTAS; que especificará las frecuencias asignadas para misiones de Comunicaciones y de Perturbación. El C-3 aprobará la lista definitiva, sin embargo el C-6 deberá mantenerla constantemente actualizándola para asegurar el máximo de efectividad de los sistemas de comunicaciones y de GE.
e. Después de todas las coordinaciones, el C-6 generará las instrucciones Operativas de Comunicaciones Electrónica (IOCE) y proveerá a las organizaciones subordinadas las frecuencias asignadas para las operaciones en curso. El planeamiento para la IOCE deberá incluir factores tales como tipos de radio disponibles en las unidades subordinadas, equipamiento criptográfico, lista de claves y frecuencias asignadas disponibles para el area de operación en particular. La compatibilidad del equipamiento será la mayor preocupación en el planeamiento de la red para sistemas de HF y VHF, en especial para las operaciones conjuntas y hasta combinadas. Así, el planeamiento debe cubrir modos de operación en salto de frecuencias y monocanal. De manera general, todas las fuerzas armadas emplean radios compatibles, pero podrían existir generaciones más antiguas o más modernas, así como equipos de otros institutos o dependencias que no cuenten con radios compatibles.
f. El planeamiento debería direccionar la interface entre radios monocanales y radios con salto de frecuencia o el emplazamiento lateral de radios compatibles en los puestos de comando. Los equipos con salto de frecuencia generalmente requieren de listas especiales de clave variables para operar en ese modo; estas variables son desarrolladas y distribuidas desde el más alto escalón posible (usualmente el C-6 u ORECOM), pero ellas deberían ser desarrolladas al más bajo escalón posible para operaciones especiales dentro de un TO.
g. El C-6 debería controlar el material criptográfico (lista de claves y aparatos) para asegurar la interoperatividad en todas los escalones, por lo que la coordinación será importante para determinar requerimientos adicionales de personal y equipo especialista.

h. La asignación de frecuencias es dependiente del área . La IOC-E debería reflejar frecuencias comunes si las unidades cambiaran sus áreas de operaciones. Todos los componentes del TO deberán proveer “entradas” sobre sus organizaciones y requerimientos especiales de comunicaciones al C-6 durante las primeras etapas del planeamiento para permitir el desarrollo y asignación de frecuencias por la IOC-E. El C-6 con estas “entradas” y aplicando el criterio pertinente interno para el cumplimiento de la misión, desarrollará la IOC-E definitiva.

135. ADMINISTRACION DEL ESPECTRO ELECTROMAGNETICO EN EL NIVEL TACTICO

a. Concepto de Administración del espectro táctico (AET)
La AET es el planeamiento sistemático, la gestión, la ingeniería y la coordinación del uso del espectro electromagnético por las unidades comprometidas en combate y en entrenamiento para el combate. En cada nivel el G-6/S-6 es el responsable ante el Cmdte por la administración del espectro, quienes designarán a un coordinador del espectro para coordinar con el escalón superior, subordinado y adyacente y con otras secciones del EM.

b. Problemas tácticos en la AET
(1) En un campo de batalla moderno, un número sin precedentes de sistemas sofisticados apoyarán al Cmdte durante la conducción de sus operaciones, muchos de los cuales son dependientes del espectro electromagnético. Muy probablemente dicho espectro, sin una adecuada administración muy rápidamente caerá en saturación y degradará seriamente el rendimiento de la misión.
(2) Tradicionalmente la administración del espectro estuvo asociada con una selección apropiada de frecuencias de operación. Hoy en día en un campo de batalla moderno, la administración del espectro debe considerar además de los sistemas de comunicaciones, a los sistemas de GE, de inteligencia, de datos, de navegación, de radar y sistemas de sensores.
(3) Constituirá un reto la automatización de la base de datos de administración de frecuencias, para que esta información llegue a ser un proceso más simple, eficiente y una tarea más fácil de ejecutar.

c. Importancia del planeamiento del espectro
(1) La misión principal de la AET es asegurar que los sistemas dependientes del espectro funcionarán conforme a su propósito de empleo. El proceso de administración no sólo se limita a proveer frecuencias asignadas, resolver conflictos y desarrollar equipos; sino que incluye también asesoramiento al Cmdte sobre los métodos para reducir las peculiaridades y/o patrones electromagnéticos de las Unidades.
(2) La coordinación con todos los escalones será clave en el proceso de administración, ya que el administrador del espectro puede reducir o evitar la interferencia perjudicial proveniente de las propias fuerzas, particularmente cuando deban conducirse operaciones de guerra electrónica.

d. Tareas funcionales de la AET
(1) En cada nivel táctico, el G-6/S-6 será responsable ante el Cmdte por la AET, en particular para cumplir las funciones básicas siguientes:

(a) Distribución proporcional de frecuencias
(b) Mantenimiento y Administración de la base de datos
(c) Resolver interferencias
(d) Evaluación de las peculiaridades y/o patrones del espectro

(2) Las subfunciones de la distribución proporcional de frecuencias son:
(a) Determinación de los requerimientos de espectro
(b) Obtención de los recursos requeridos
(c) Balance de recursos disponibles versus lo requerido
(d) Distribución priorizada y proporcional de recursos al usuario
(e) Evaluación y optimización del uso del espectro.

(3) Los requerimientos del espectro para el combate están determinados por las necesidades operacionales del usuario. El administrador del espectro, basado en la doctrina y en su experiencia, deberá hacer una buena apreciación de los requerimientos de la unidad. La operación y el equipo disponible determina el requerimiento actual. Estos datos son extraídos de las órdenes de operaciones, los POV´s y de la coordinación con los G-6´s/S-6´s de las GGUU/Unidades. Los datos pueden ser categorizados de la siguiente manera:
(a) VHF-FM
(b) VHF-AM
(c) UHF-AM
(d) UHF-FM
(e) HF (onda terrestre)
(f) HF (onda espacial)
(g) Comunicaciones multicanal
(h) Comunicaciones satelitales
(i) Frecuencias de radar
(j) Frecuencias de perturbadores
(k) Frecuencias para tierra-aire
(l) Frecuencias para enlace de datos
(m) Frecuencias para sistemas de distribución de datos
(n) Frecuencias de ayuda de navegación
(ñ) Frecuencia de sensores
(o) Frecuencia de armas dirigidas con energía electromagnética

(4) Restricciones de frecuencia para formar redes.- Todos los radios para una red particular deben ser capaces de operar en la misma frecuencia. Las frecuencias de red deben asignarse con la consideración principal de las capacidades de sintonización de las radios de serie antigua, como por ejemplo la serie de VHF-FM que posee un canal cada 100 Khz y las que tiene 50 Khz; con los de última tecnología cada 25 Khz. Cuando se forma una red de radios deben considerarse estas diferencias.

(5) En cuanto a la obtención de recursos de frecuencia, normalmente un EO recibe sus recursos de la autoridad de administración del espectro del TO y una GU lo recibe del EO. Inicialmente el planificador de frecuencias identifica sus requerimientos y lo siguiente será obtener los recursos necesarios; para ello debe hacerse cada esfuerzo para obtener y trasladar los recursos con las mínimas restricciones para permitir a los usuarios la máxima flexibilidad.

(6) El balance se logra mediante la coordinación, reparto, adjudicación y asignación:

(a) La coordinación es un proceso continuo y será esencial para un programa efectivo de administración del espectro.
(b) El reparto es el establecimiento de bandas de frecuencia para funciones específicas o servicios de radio tales como radiodifusión, fijo y móvil. Cuando se autoriza más de un tipo de servicio en una banda, el rango de servicios va de principal, permitido o secundario. El principal y el permitido tendrán iguales derechos excepto en la preparación de los planes de frecuencia. El servicio principal tiene la primera opción en la elección de frecuencias y los servicios secundarios son la base de no-interferencia.
(c) La adjudicación es el establecimiento de bandas específicas o frecuencias dentro de una banda prescrita adjudicada nacional e internacionalmente.
(d) La asignación es la autorización dada por la autoridad apropiada para una estación de radio para usar una RF o canal de radio bajo condiciones especificadas. La asignación es el método principal de balancear los recursos disponibles de frecuencias versus los requerimientos.

(7) La distribución priorizada y proporcional se realiza a través de la IOC-E para VHF-FM, VHF-AM y UHF-AM. Para las otras frecuencias se emplearán formatos específicos para cada tipo o categoría.
(8) Una revisión constante optimizará el uso del espectro, analizándose en todo momento la eficiencia del sistema de red, la efectividad del uso del espectro y los cambios en la misión de la unidad; asegurando al cmdte táctico que reciba el apoyo requerido.

136. TAREAS FUNCIONALES BASICAS DE LA ADMINISTRACION DEL ESPECTRO TACTICO

a. Distribución proporcional de frecuencias
(1) A nivel división serán identificados muchos requerimientos, los que serán pasados al administrador del espectro de la división. Si éste no tiene los recursos de frecuencias suficientes para satisfacer los requerimientos, los solicitará al administrador del espectro del EO. De la misma forma si este último no los posee, los trasladará al administrador del TO.
(2) Los requerimientos del espectro deben ser determinados tan pronto como sea posible durante el planeamiento de una operación o durante las etapas de desarrollo del equipamiento (o procesos de adquisición). La obtención de recursos de frecuencias puede ser un proceso complejo y que consume tiempo (desde algunos días hasta meses), que incluso puede tomar años coordinarlo.
(3) La precisión de una solicitud de frecuencia puede hacer la diferencia entre el éxito o fracaso de una misión. El solicitante debe asegurar que todos los datos necesarios estén incluidos y sean los correctos. Estos datos incluyen designadores de emisión y clase de estación. Luego el solicitante debe justificar que el requerimiento es esencial para su misión, ya que los administradores deberán insistir del porque de la necesidad y como será usado la frecuencia, pues los canales de coordinación podrían volverse demasiado lentos y tediosos sino se

logra la credibilidad absoluta en cuanto lo importante para una opn de la frecuencia solicitada.

(4) Las características técnicas del equipo son necesarias para prorratear el espectro y para resolver interferencias. Estas características incluyen rango de sintonía, emisión, canalización y método de sintonía. Las salidas del proceso de distribución proporcional (tales como las IOC-E, diagramas multicanal y otros registros de uso de frecuencias) serán la base para un completo concepto de una administración efectiva del espectro táctico.

b. Administración de la base de datos

(1) A través de la base de datos, el administrador del espectro debería tener una lista completa de equipos dependientes del espectro electromagnético en su área de responsabilidad. En este punto, una base de datos del administrador del espectro puede incluir:
- registros de frecuencias asignadas
- documentos conteniendo parámetros de señal de los equipos.
- Tablas de reparto de frecuencias
- Listas de equipos
- Indices
- Documentos de reparto de equipos
- Regulaciones nacionales (DGT) e internacionales (UIT)
- Normas y directivas del CCFA y del ejército
- Manuales y boletines

(2) Todos estos registros y documentos que podrían formar parte de la base de datos, deberán ser mantenidos al día, inicialmente de manera manual; sin embargo constituirá un reto la automatización de todos ellos para llegar a convertirse en la norma antes que la excepción.

c. Resolución de interferencias

(1) La solución de interferencias debe ser manejado al más bajo nivel posible. El administrador del espectro es la autoridad final de la solución. La interferencia puede provenir de aparatos de Telemática (radios y radares propios o no de manera no-intencional) y de aparatos de motores (vehículos, compresoras, aparatos de soldadura, etc).

(2) Después de que se le informe de alguna interferencia no solucionada, el administrador del espectro o el G-6/S-6 puede:
(a) Buscar el asesoramiento del Oficial de guerra electrónica para la identificación de la fuente
(b) Recomendar la reubicación física del afectado
(c) Recomendar, tolerar la interferencia (trabajar a pesar de ella)
(d) Realizar cambios apropiados en las asignaciones.

(3) El Oficial de GE puede detectar la interferencia hostil a la perturbación antes de que sea reconocida e informada al administrador del espectro. En tales casos, la coordinación de la interferencia debería ser iniciada al contrario para asegurar que las funciones de Telemática inefectivas sean reconocidas y corregidas; para lo cual el informe MIPIS puede ser el iniciador. Este informe se envía por los canales de administradores del espectro para que determinen si la interferencia pudiera ser no-intencional o intencional; en este último caso se transfiere al elemento de GE para su acción correspondiente.

(4) Todo operador de algún equipo que emite o recibe Telemática debe ser capaz de discernir si la interferencia proviene de algún fenómeno natural o de fuente producida por el hombre. En el primer caso, el operador debería tratar de trabajar a pesar de la interferencia, si aun la persistencia de esa interferencia es intolerable se coordinará para el cambio. En el segundo caso, el operador verifica internamente su equipo para eliminar posibles causas debido al mal funcionamiento del mismo, tales como descalibraciones, componentes degradados, desorientación de antena o pobre mantenimiento; si ninguna de estas u otras causas son encontradas en el propio equipo, se verificará el área y/o la red para encontrar incompatibilidades; si se persiste en la interferencia o no se identifica la fuente se elabora el informe MIPIS para el administrador del espectro y para el centro de GE conjunto; quienes trabajarán para minimizar los efectos y/o detectar la fuente.

(5) De una manera general, lo aquí expuesto es un procedimiento para la solución de problemas de interferencias que puedan incumbir al administrador del espectro. Mayores detalles sobre la resolución se podrán encontrar en el Manual de Administración de Frecuencias.

d. Evaluación de las peculiaridades y/o patrones del espectro

(1) Una peculiaridad del espectro es un patrón distintivo de emanaciones espectrales de un aparato o reunión de aparatos. Estos aparatos incluyen equipos de Telemática (comunicaciones, radares, etc.), generadores de potencia, motores de vehículos, equipos de soldadura, compresoras y la radiación de las facilidades/instalaciones de los PC´s.

(2) Un patrón es formado por algunas variables: tiempo del día, área geográfica, número, tipo, frecuencia y potencia del emisor. Estas variables conforman una peculiaridad electromagnética identificable.

(3) El administrador del espectro es el punto de contacto para tratar las vulnerabilidades de las peculiaridades electromagnéticas. Esto es una parte de sus responsabilidades como Oficial de Control de emisiones, que también incluye considerar las emanaciones de calor provenientes de los monoblocks de los motores que de los aparatos infrarrojos pudieran detectar. El control de emisiones (CONEM) y la implementación efectiva de la protección electrónica (antes COCOME) son las responsabilidades del administrador del espectro.

(4) El objetivo de la evaluación de las peculiaridades del espectro es evaluar el grado en el cual las facilidades/instalaciones de la Unidad/GU, son identificables por su peculiaridad y para asesorar al Cmdte la manera como se puede eliminar, proteger, disimular o enmascarar esa vulnerabilidad.